Universidad Estatal «M.V. Lomonósov» de Moscú

LIBRO DE TEXTO UNIVERSITARIO CLÁSICO

A. N. Kolmogórov, A. G. Dragalin

LÓGICA MATEMÁTICA

Capítulos complementarios

URSS

А. Н. Колмогоров, А. Г. Драгалин

МАТЕМАТИЧЕСКАЯ ЛОГИКА

Дополнительные главы

НАУКА

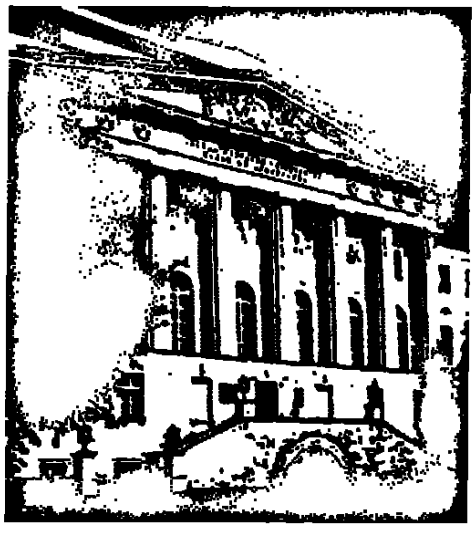
РОССИЯ – МИРУ

Serie

LIBRO DE TEXTO UNIVERSITARIO CLÁSICO

instituida en el año 2002 por iniciativa del rector de la Universidad Estatal «M. V. Lomonósov» de Moscú, V. A. Sadóvnichi, en conmemoración del

250 Aniversario de la Universidad de Moscú



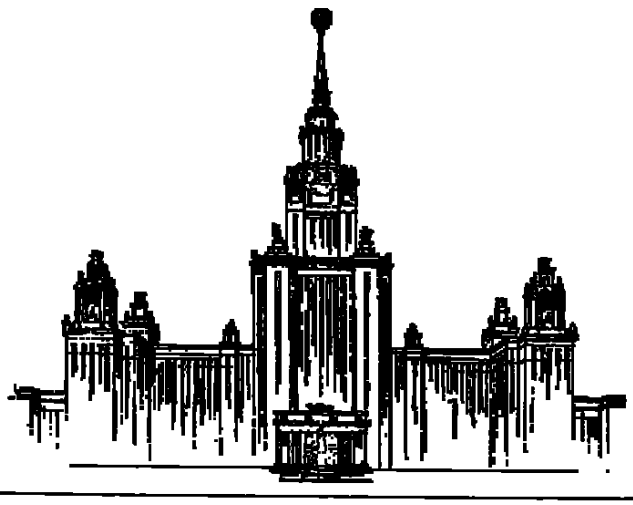
LIBRO DE TEXTO UNIVERSITARIO CLÁSICO

Consejo de Redacción de la Serie

Presidente del Consejo,
rector de la Universidad de Moscú,
V. A. Sadóvnichi

Miembros del Consejo:

Vijanski O. S., Golíchenkov A. K., Gúsiev M. V.,
Dobrenkov V. I., Dontsov A. I., Zasurski Ya. N., Zínchenko Yu. P.
(secretario ejecutivo), Kamzólov A. I. (secretario ejecutivo),
Kárpov S. P., Kasímov N. S., Kóliesov V. P., Lobodánov A. P.,
Lunin V. V., Lupánov O. B., Méier M. S., Mirónov V. V.
(vicepresidente), Mijaliov A. V., Moisiéev Ye. I.,
Puscharovski D. Yu., Raiévskaia O. V., Remniova M. L.,
Rózov N. J., Salietski A. M. (vicepresidente), Surin A. V.,
Ter-Minásova S. G., Tkachuk V. A., Tretiakov Yu. D., Trujin V. I.,
Trofímov V. T. (vicepresidente), Shoba S. A.



Universidad Estatal «M.V. Lomonósov» de Moscú
Московский государственный университет им. М. В. Ломоносова

А. Н. Колмогоров, А. Г. Драгалин
МАТЕМАТИЧЕСКАЯ ЛОГИКА
ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ

A. N. Kolmogórov, A. G. Dragalin

LÓGICA MATEMÁTICA

CAPÍTULOS COMPLEMENTARIOS

Aprobado por el
Ministerio de Educación Superior y Especial Media de la URSS
como libro de texto para estudiantes de las especialidades
de matemática de centros de formación superior

URSS
MOSCÚ

Andréi Nikoláievich Kolmogórov,
Alekséi Grigórievich Dragalin

Lógica matemática. Capítulos complementarios.

A. N. Kolmogórov y A. G. Dragalin, eminentes lógicos y matemáticos soviéticos, ejercieron una marcada influencia en el estilo y la dirección de las investigaciones en el campo de la lógica y la filosofía matemática a nivel mundial.

El presente libro constituye el segundo tomo de la obra «Lógica matemática» (el primer tomo, «Introducción a la lógica matemática», también fue editado por nuestra editorial), en la que se da una exposición clásica de los conceptos y resultados fundamentales de la lógica matemática con elementos de teoría de conjuntos, teoría de algoritmos y fundamentos de la matemática. Ambos tomos fueron escritos sobre la base del curso de lógica matemática dictado por los autores en la Facultad de Mecánica y Matemática de la Universidad Estatal «M. V. Lomonósov» de Moscú.

En el primer capítulo del presente libro se estudia la teoría de conjuntos sobre la base del sistema axiomático de Zermelo—Fraenkel. El segundo capítulo es una introducción a la teoría de algoritmos (computabilidad según Turing, tesis de Church, conjuntos recursivos, conjuntos recursivamente enumerables). El tercer capítulo está dedicado a la teoría de la deducción (teorema de completitud del cálculo de predicados de Gödel, teorema de Löwenheim—Skolem, segundo teorema de Gödel) y concluye con el examen del programa de Hilbert de fundamentación de la matemática.

Este libro está dirigido a lectores de nivel universitario interesados en la lógica matemática y los problemas filosóficos de la matemática moderna.

Traducido del ruso por Carlos Daniel Navarro Hernández (Licenciado en Ciencias Físico-matemáticas) y Juan Enrique Palomino Pérez (Ingeniero)

Издательство «КРАСАНД». 117335, Москва, Нахимовский пр-т, 56.
Формат 60×90/16. Печ. л. 15.

Отпечатано в ООО «Ульзама Дихиталь». 31620, Уартэ, пром. зона «Арэта», А-33.

ISBN 978–5–396–00072–8

© KRASAND, 2013

7989 ID 108167

9 785396 000728

HAYKA
LIBROS DE CIENCIA
Distribuidor exclusivo en España de Grupo URSS
• e-mail: HAYKA@haykalibros.es
tel./fax: +34 (954)71 98 62
móvil: +34 (625)37 87 73
• http://URSS.ru
e-mail: URSS@URSS.ru
tel./fax: + 7(499)724 25 45
URSS

Impreso en España

Reservados todos los derechos en todas las lenguas y en todos los países del mundo. Quedan rigurosamente prohibidas, sin la autorización escrita de los titulares del «Copyright», bajo las sanciones establecidas en las leyes, la reproducción total o parcial de esta obra por cualquier medio o procedimiento (comprendidos la reprografía, el tratamiento informático y la exposición en Internet) y la distribución de ejemplares de ella mediante alquiler o préstamo público.

Índice

Prólogo a la serie 7

Prólogo 9

Introducción 12

Capítulo 1
Teoría de conjuntos 27

1.1. Lenguaje de la teoría ingenua de conjuntos. Paradojas de la teoría ingenua de conjuntos 29

1.2. Lenguaje de la teoría de conjuntos de Zermelo—Fraenkel 45

1.3. Relaciones y función en el lenguaje de la teoría de conjuntos 51

1.4. Los números naturales en la teoría de conjuntos. Escritura de las afirmaciones matemáticas en el lenguaje de la teoría de conjuntos 66

1.5. Sobre la hipótesis del continuo y el axioma de elección . . . 80

1.6. Teoría axiomática de conjuntos de Zermelo—Fraenkel . . . 85

Capítulo 2

Elementos de teoría de algoritmos **105**

2.1. Máquinas de Turing 107

2.2. Tesis de Church 123

2.3. Conjuntos y predicados recursivos y recursivamente enumerables 126

2.4. Funciones recursivas primitivas. Numeración de Gödel. Aritmética con términos recursivos primitivos 140

2.5. Algunos teoremas de la teoría general de algoritmos 155

Capítulo 3

Elementos de teoría de la demostración **169**

3.1. Incompletitud e indecidibilidad de las teorías axiomáticas 171

3.2. Teorema de Gödel de completitud del cálculo de predicados 187

3.3. Teorema de eliminación del corte 200

3.4. Sobre el programa de Hilbert de fundamentación de la matemática 215

Bibliografía **227**

Índice de autores **229**

Índice de materias **231**

Prólogo a la serie

Estimado lector:

La obra que usted tiene en sus manos forma parte de la serie «Libro de texto universitario clásico», publicada en conmemoración del 250 Aniversario de la Universidad Estatal «M. V. Lomonósov» de Moscú. Esta serie comprende más de 150 libros de texto, recomendados por los Consejos Científicos de las Facultades de la Universidad y por el Consejo de Redacción de la serie y aprobados por el Consejo Científico de la Universidad Lomonósov.

La Universidad «M. V. Lomonósov» siempre se ha caracterizado por la alta cualificación de su cuerpo de profesores, quienes han educado a numerosas generaciones de estudiantes, los cuales a su vez han hecho importantes aportes al desarrollo de la ciencia y la cultura, tanto en Rusia como a nivel mundial.

El alto nivel de la enseñanza ofrecida por la Universidad Lomonósov es garantizado, en primer lugar, por el alto nivel de los libros de texto y manuales utilizados en ella, los cuales han sido escritos por eminentes científicos y pedagogos, y combinan en sí la profundidad y la accesibilidad del material presentado. Estos libros acumulan la valiosa experiencia alcanzada en la metodo-

logía de la enseñanza, que de esta forma deja de ser propiedad exclusiva de la Universidad Lomonósov para convertirse en parte del patrimonio pedagógico de otras universidades de Rusia y del mundo.

La edición de la serie «Libro de texto universitario clásico» es muestra patente del aporte realizado por la Universidad Lomonósov a la enseñanza universitaria clásica en nuestro país y, sin duda, contribuirá a su desarrollo.

La realización de esta noble tarea hubiera sido imposible sin la participación activa de las editoriales que la han hecho realidad. Nuestra institución valora altamente esta colaboración en apoyo de la posición que hemos mantenido en el campo de la ciencia y la enseñanza. Asimismo, esto demuestra que el 250 Aniversario de la Universidad «M. V. Lomonósov» de Moscú es un hecho de importancia trascendental para toda Rusia y la comunidad pedagógica mundial.

Rector de la Universidad Estatal
«M. V. Lomonósov» de Moscú,
Académico AC de Rusia,
Profesor

V. A. Sadóvnichi

Prólogo

Este libro fue ideado, junto con [11], como un primer curso de lógica matemática, escrito sobre la base de las lecciones dictadas por los autores como parte del curso (de un semestre) de lógica matemática impartido a los estudiantes del primer curso de la Facultad de Mecánica y Matemática de la Universidad Lomonósov de Moscú. El objetivo de los autores es dar a conocer al lector los conceptos fundamentales de la lógica matemática, los cuales son de importancia para los matemáticos de cualquier especialidad. Se dedica una gran atención al uso correcto de las notaciones exactas utilizadas en la lógica matemática para la escritura de las afirmaciones matemáticas, así como a las leyes lógicas, los fundamentos de la teoría de conjuntos y la teoría de algoritmos.

El presente libro es la continuación del curso y puede leerse independientemente de [11] si el lector cuenta con conocimientos preliminares sobre los lenguajes lógico-matemáticos y cierta práctica en la deducción lógica. Los conocimientos básicos necesarios se pueden encontrar en [11] o en los primeros capítulos de cursos más detallados de lógica matemática (por ejemplo, [9, 10, 14]). El mínimo de conocimientos necesario será dado en la introducción del presente tomo.

En el primer capítulo se estudia la teoría de conjuntos sobre la base del sistema axiomático de Zermelo—Fraenkel. El objetivo es mostrar cómo se pueden introducir los principales conceptos matemáticos y estructuras sobre la base del lenguaje lógico-matemático exacto de la teoría de conjuntos. Aquí se tratan algunos temas tradicionales relacionados con los fundamentos de la teoría de conjuntos, como son las paradojas de la teoría de conjuntos, la consistencia del sistema de Zermelo—Fraenkel, la paradoja de Skolem, los métodos axiomáticos informal y formal en la matemática.

En el segundo capítulo se estudian los elementos de la teoría de algoritmos. Se dan las definiciones exactas relacionadas con la computabilidad según Turing, se discuten la tesis de Church y los conceptos de conjunto recursivo y conjunto recursivamente enumerable. Esta parte del capítulo puede considerarse como el mínimo de conocimientos necesarios sobre teoría de algoritmos. Más adelante se enuncian los principales teoremas de la teoría general de algoritmos sobre la existencia de conjuntos y predicados indecidibles, y se da el material preparatorio relacionado con la numeración de Gödel de objetos constructivos y con las propiedades de los objetos constructivos en la aritmética formal. Esta temática puede impartirse en clases facultativas; el profesor puede utilizarlo de manera selectiva o impartir ciertos temas durante las clases prácticas.

El tercer capítulo está dedicado a la teoría de la deducción. Se demuestra el teorema de completitud del cálculo de predicados perteneciente a Gödel, el teorema de Löwenheim—Skolem y el teorema de incompletitud e indecidibilidad de toda teoría axiomática suficientemente expresiva. Se demuestra también el segundo teorema de Gödel sobre la imposibilidad de demostrar

la consistencia de una teoría axiomática suficientemente potente utilizando medios de esta misma teoría, así como el teorema de Gentzen sobre la eliminación del corte. El capítulo concluye con el examen del programa de Hilbert de fundamentación de la matemática. El material de este capítulo también puede considerarse como facultativo. Por ejemplo, el profesor puede limitarse a la formulación de los teoremas más importantes.

En el libro se utilizan las siguientes notaciones. El símbolo ▶ indica el inicio de una demostración, mientras que el símbolo ◀, su final. Los signos $\leftrightharpoons$, $\Rightarrow$, $\Leftrightarrow$ sustituyen las frases «por definición», «si..., entonces», «si y sólo si», respectivamente.

La mayor dificultad con que se enfrenta la enseñanza de la lógica matemática consiste en que la demostración rigurosa de los resultados más importantes exige el conocimiento de un vasto aparato preliminar. Por ejemplo, es necesario convencerse de que unos u otros predicados realmente son computables según Turing o recursivos primitivos, o demostrar, digamos, que las fórmulas en cuestión son deducibles en una u otra teoría axiomática formal. Este tipo de afirmaciones se demuestran habitualmente mediante la construcción (voluminosa, pero en esencia simple) de las correspondientes máquinas de Turing, descripciones recursivas primitivas, deducciones formales, etcétera. Por supuesto, si el curso es corto, no tiene sentido dedicarse a estas construcciones. Si el lector está interesado en los detalles, puede remitirse a libros de texto más extensos. De todos modos, hemos tratado en la medida de lo posible de presentar detalladamente los momentos esenciales en todas las demostraciones.

A. N. Kolmogórov
A. G. Dragalin

Introducción

Recordemos algunas definiciones y conceptos que serán necesarios en lo sucesivo. Una exposición detallada se ofrece, por ejemplo, en [11]. Este material también se encuentra en los primeros capítulos de libros destinados a especialistas en lógica matemática (véanse [10, 14]).

En la lógica, los enunciados matemáticos se expresan como fórmulas escritas en lenguajes lógico-matemáticos definidos exactamente. Los objetos fundamentales de un lenguaje lógico-matemático son las *expresiones*. Las expresiones se dividen en *fórmulas* y *términos*. Un lenguaje Ω contiene varios tipos de variables. Las variables de cada tipo se consideran como variables que recorren cierta región: un conjunto de objetos de un tipo dado. Las apariciones de las variables en las expresiones de un lenguaje se dividen en *libres* y *ligadas*. Las variables que aparecen libres en una expresión se denominan *parámetros* de esta expresión. Una expresión que no contiene parámetros se denomina *cerrada*.

Las expresiones de un lenguaje lógico-matemático son filas de símbolos-letras del alfabeto del lenguaje dado, y se construyen de acuerdo con ciertas reglas definidas rigurosamente.

Cada fórmula C del lenguaje Ω puede tener una y sólo una de las siguientes siete formas:

$(A \wedge B)$ — se lee «A y B»;

$(A \vee B)$ — se lee «A o B»;

$(A \supset B)$ — «de A se deduce B»;

$\neg A$ — «no A»;

$\forall x A$ — «para todo x tiene lugar A»;

$\exists x A$ — «existe un x tal que A» es una fórmula atómica.

Los símbolos $\wedge$, $\vee$, $\supset$ y $\neg$ se denominan *conectivas lógicas*, y sus nombres son *conjunción*, *disyunción*, *implicación* y *negación*, respectivamente. Los símbolos $\forall$ y $\exists$ se denominan *cuantificadores universal* y *cuantificador existencial*, respectivamente. Como de costumbre, se considera que los prefijos cuantificantes $\forall x$ y $\exists x$ ligan a la variable x en la fórmula que sigue, de modo que si una fórmula comienza con uno de estos prefijos, la variable x no aparecerá libre en ella.

La construcción de las fórmulas atómicas depende del lenguaje considerado. Las fórmulas atómicas se forman de una manera particularmente sencilla en los *lenguajes de primer orden*, que constituyen el objeto fundamental de estudio en la lógica matemática. Concretamente, toda fórmula atómica en un lenguaje de primer orden tiene la forma $P(t_1, \ldots, t_n)$, donde P es una *letra de predicado* de este lenguaje, y $t_1, \ldots, t_n$ son términos del lenguaje. No se excluye el caso $n = 0$, es decir, toda letra de predicado 0-ádica es una fórmula atómica; en este caso se denomina *letra proposicional*, o *variable proposicional*. Una letra de predicado n-ádica representa en el lenguaje un *predicado*

de n variables (en otra terminología, *enunciado paramétrico, forma proposicional* de n variables).

En diferentes lenguajes los términos están formados de diferentes maneras. Aquí también el caso más sencillo e importante es el de los lenguajes de primer orden. En estos lenguajes los términos se construyen a partir de variables y constantes del lenguaje con ayuda de los *símbolos de función*, es decir, todo término es, o bien una variable, o bien una constante del lenguaje, o bien tiene la forma $f(t_1, \ldots, t_n)$, donde f es un símbolo de función que denota una operación n-ádica en el lenguaje. En los lenguajes de primer orden todas las variables que forman un término son libres, es decir, son parámetros de este término.

En la práctica, cuando se escriben las fórmulas y términos se «economizan» paréntesis, para lo que aplicamos convenios bien conocidos. Por ejemplo, habitualmente se omiten los paréntesis externos. Además, las conectivas lógicas y los cuantificadores se sitúan en un orden determinado considerando que los símbolos que en este orden se encuentran a la derecha «ligan más fuerte», es decir, ellos deben ser ejecutados en primer lugar. Para evitar confusión, seguiremos el siguiente orden de ejecución de las operaciones:

$$\equiv \supset \begin{matrix} \vee \\ \wedge \end{matrix} \neg \begin{matrix} \forall \\ \exists \end{matrix}.$$

Aquí, $\equiv$ es una conectiva lógica derivada que se define a partir de las ya mencionadas: $A \equiv B$ es una notación abreviada para la fórmula $((A \supset B) \wedge (B \supset A))$.

Por ejemplo, la fórmula

$$(\forall x(P(x, y) \supset (\forall z Q(z) \wedge R)) \vee Q(x))$$

se puede escribir en la forma

$$\forall x(P(x, y) \supset \forall z Q(z) \wedge R) \vee Q(x).$$

A veces, para economizar paréntesis utilizamos un punto. Si dentro de un par de paréntesis se ejecutan varios símbolos homogéneos (según su fuerza de ligación), entonces un punto junto a un símbolo indica el *símbolo lógico principal*, es decir, aquél que se ejecuta en último lugar. Por ejemplo, la fórmula

$$P \supset (Q \vee R \equiv (\neg R \equiv \neg P))$$

se puede escribir en la forma

$$P \supset (Q \vee R \equiv. \neg R \equiv \neg P).$$

Sea T una expresión del lenguaje. Sean $x_1, \ldots, x_n$ variables diferentes y $t_1, \ldots, t_n$ términos de los tipos correspondientes. Mediante $(T(x_1, \ldots, x_n \parallel t_1, \ldots, t_n))$ denotamos el *resultado de la sustitución correcta* de los términos $t_1, \ldots, t_n$ en lugar de las apariciones libres de las variables $x_1, \ldots, x_n$ en la expresión T. Para obtener la expresión $(T(x_1, \ldots, x_n \parallel t_1, \ldots, t_n))$ se deben sustituir simultáneamente todas las apariciones libres de las variables $x_1, \ldots, x_n$ por los términos $t_1, \ldots, t_n$, respectivamente. Además, si es necesario, se deben renombrar algunas variables ligadas de la expresión T. Concretamente, si en un término t_i una variable x (inicialmente libre en t_i) resulta ligada después de la sustitución (en estos casos se dice que en el término t_i tiene lugar una *colisión* de variables), entonces en T preliminarmente se deben renombrar algunas variables ligadas por nuevas de modo que después de la sustitución no ocurran

colisiones. Por ejemplo, el resultado de la sustitución correcta

$$(\exists\, xP(x,y)(y \parallel f(x,y)))$$

es la fórmula

$$\exists\, uP(u, f(x,y)),$$

con la nueva variable ligada u.

Simplificamos la expresión $(T(x_1,\ldots,x_n \parallel t_1,\ldots,t_n))$ y obtenemos $T(x_1,\ldots,x_n \parallel t_1,\ldots,t_n)$, o incluso $T(t_1,\ldots,t_n)$ si mencionar las variables $x_1,\ldots,x_n$ no es esencial. Debemos recordar que en las notaciones de la forma $A(t,r)$ siempre se tiene en cuenta una sustitución correcta con el requerido renombramiento de las variables ligadas.

Nosotros suponemos que el lector conoce los lenguajes de primer orden más habituales: el lenguaje de la aritmética, el lenguaje de la teoría de grupos, el lenguaje de la lógica de predicados. El lenguaje de la lógica de predicados y el lenguaje de la aritmética volverán a ser tratados posteriormente.

Las expresiones de un lenguaje son simplemente filas de símbolos de tipo especial y no tienen ningún sentido por sí mismos. Para que el lenguaje Ω adquiera sentido es necesario definir una *interpretación* para el lenguaje Ω (en otra terminología, *estructura para el lenguaje* Ω). Definir una interpretación M del lenguaje Ω significa, en particular, definir una *región de variación* para cada tipo de variable presente en el lenguaje. Si en una expresión arbitraria del lenguaje se sustituyen todos los parámetros por objetos de las respectivas regiones de variación, entonces se obtiene lo que se denomina *expresión valorada* del lenguaje (más exactamente, expresión valorada en un modelo dado M). En particular, una expresión cerrada es valorada en cualquier modelo.

Toda interpretación M de un lenguaje permite dividir según reglas naturales todas las fórmulas valoradas en *verdaderas* en la interpretación dada y *falsas* en la interpretación dada. Si A es una fórmula valorada en M, entonces la notación $M \models A$ significa que A es verdadera en la interpretación M.

El concepto de *veracidad* de una fórmula valorada en una estructura M está estrechamente relacionado con la estructura de la fórmula. Por ejemplo,

$$M \models A \wedge B$$

si y sólo si $M \models A$ y $M \models B$. Asimismo, $M \models A \vee B$ si y sólo si $M \models A$ o $M \models B$; $M \models \neg A$ si y sólo si no es válido $M \models A$. La afirmación $M \models A \supset B$ es falsa solamente en un caso, a saber, cuando $M \models A$ y $M \models \neg B$. Para las demás combinaciones de valores veritativos, la afirmación $M \models A \supset B$ se considera verdadera (la conectiva lógica $\supset$ interpretada de esta manera es denominada a menudo *implicación material*). A continuación, $M \models \forall x A$ si y sólo si para todo objeto a de la región de variación de la variable x se cumple $M \models A(x \parallel a)$. De modo similar, $M \models \exists x A$ si y sólo si existe un objeto a de la región necesaria tal que $M \models A(x \parallel a)$. Brevemente, se puede decir que hemos adoptado la semántica clásica, donde las conectivas lógicas se interpretan según las leyes del álgebra booleana binaria.

De manera similar, la interpretación M permite atribuir un valor $|t|_M$ a cada término valorado del lenguaje. El valor $|t|_M$ es un objeto que expresa el término t para una valoración dada de sus parámetros. El valor de un término sólo depende de los valores de los subtérminos que lo forman. Esto significa que si r es un término cuyos parámetros, a excepción, posiblemente,

de x, han sido valorados, y t es un término valorado del mismo tipo que x, entonces $|(x \parallel t)|_M$ coincide con $|r(x \parallel |t|_M)|_M$.

Igualmente, $M \models A(x \parallel t)$ si y sólo si $M \models A(x \parallel |t|_M)$.

De esta manera, para una interpretación dada M del lenguaje Ω, la fórmula A de este lenguaje se considera como una fórmula que expresa cierto enunciado paramétrico que depende de la valoración de los parámetros. En este caso se dice que la fórmula define en Ω una *forma proposicional*. En particular, si una fórmula es una sentencia de Ω, es decir, no contiene parámetros, entonces esta fórmula define en M una proposición concreta, verdadera o falsa. De modo análogo, el término t define en M una operación con sus parámetros. Un término cerrado define en la interpretación M un objeto concreto.

Desde el punto de vista de la lógica, son de especial interés las fórmulas del lenguaje que son verdaderas en toda interpretación de Ω para cualquier valoración de sus parámetros. Estas fórmulas se denominan *leyes lógicas* del lenguaje (en otra terminología, *tautologías* del lenguaje). El concepto de *ley lógica* es una idea matemática de carácter más específico que el concepto de *fórmula* (una fórmula es verdadera «en virtud de su propia forma, independientemente de su contenido»).

Diremos que una fórmula A es lógicamente equivalente a una fórmula B (escribimos $A \sim B$) si la fórmula $A \equiv B$ es una ley lógica. Indudablemente, el lector conoce algunas leyes y equivalencias lógicas, como la expresión de unas conectivas lógicas mediante otras, la introducción de los cuantificadores a través de las conectivas lógicas, etcétera. Las leyes lógicas permiten transformar las fórmulas en la forma que necesitamos. Por ejemplo, como se sabe, toda fórmula puede ser sustituida

por una fórmula lógicamente equivalente que tiene *forma prenexa*, es decir, una fórmula en la que todos los cuantificadores se encuentran delante.

Para cada lenguaje lógico-matemático Ω se define el *cálculo de predicados* en el lenguaje Ω. Para describir el cálculo de predicados, se definen sus axiomas y reglas de inferencia. Cabe señalar que las formulaciones encontradas en diferentes libros de texto pueden diferenciarse una de otra (por supuesto, estas diferencias no son esenciales para la teoría que se desarrolla a continuación). Nosotros adoptaremos la siguiente formulación. Denominaremos *axiomas del cálculo de predicados* en el lenguaje Ω a las fórmulas de este lenguaje que poseen una de las siguientes formas:

1) $A \supset . B \supset A$;
2) $(A \supset . B \supset C) \supset . (A \supset B) \supset (A \supset C)$;
3) $A \supset . B \supset A \wedge B$;
4) $A \wedge B \supset A$;
5) $A \wedge B \supset B$;
6) $(A \supset C) \supset . (B \supset C) \supset (A \vee B \supset C)$;
7) $A \supset A \vee B$;
8) $B \supset A \vee B$;
9) $(A \supset B) \supset . (A \supset . \neg B) \supset \neg A$;
10) $\neg\neg A \supset A$;
11) $\forall x A \supset A(x||t)$;
12) $\forall x(C \supset A(x)) \supset . C \supset \forall x A(x)$;
13) $A(x||t) \supset \exists x A$;
14) $\forall x(A(x) \supset C) \supset . \exists x A(x) \supset C$.

Aquí, A, B, C son fórmulas arbitrarias de Ω. En los esquemas 12 y 14, la fórmula C no contiene apariciones libres de la variable x. No es difícil verificar que todos los axiomas del cálculo de predicados son leyes lógicas.

Las *reglas de inferencia* del cálculo de predicados son figuras de las siguientes formas:

$$\frac{A, A \supset B}{B}, \quad \frac{A}{\forall x A}.$$

Aquí, A, B son fórmulas arbitrarias de Ω, x es una variable arbitraria. La primera lleva el nombre tradicional latín de *regla modus ponens*; la segunda regla se denomina *regla de generalización*.

Un *árbol de fórmulas* es, por definición, una figura bidimensional formada por fórmulas del lenguaje según las siguientes reglas:

1) Toda fórmula A es un árbol de fórmulas, y la fórmula inferior de este árbol es la propia fórmula A.
2) Si D_1 y D_2 son árboles de fórmulas con fórmulas inferiores de las formas A y $A \supset B$, respectivamente, entonces la figura
$$\frac{D_1, D_2}{B}$$
es un árbol de fórmulas. En este caso, decimos que la fórmula B se obtiene en este árbol a partir de A y $A \supset B$ según la regla modus ponens. La fórmula inferior del árbol resultante de fórmulas es, por definición, la fórmula B.
3) Si D_1 es un árbol de fórmulas con fórmula inferior A, y x es una variable, entonces la fórmula
$$\frac{D_1}{\forall x A}$$

también es un árbol de fórmulas. En este caso, decimos que la fórmula inferior $\forall x A$ de este árbol de fórmulas se obtiene de A según la regla de generalización.

Resumiendo, un árbol de fórmulas es un árbol finito en cuyos vértices se tienen fórmulas, y en el cual el movimiento de arriba hacia abajo se efectúa según las reglas de inferencia del cálculo de predicados.

Las fórmulas iniciales (superiores) de un árbol de fórmulas *que no tienen forma de axiomas del cálculo de predicados* se denominan *hipótesis*, o bien *premisas abiertas*, del árbol de fórmulas considerado. Llamaremos *rama* de un árbol de fórmulas D a toda sucesión $A_1, \ldots, A_n$ de apariciones de fórmulas en D tal que para todo $i < n$ la fórmula A_{i+1} se encuentra inmediatamente encima de la fórmula A_i en D, y A_1 es la fórmula inferior y A_n es la fórmula superior de D. Sean A y B diferentes ocurrencias de las fórmulas en D. Diremos que la fórmula B es *superior* a la fórmula A en el árbol D si existe una rama $A_1, \ldots, A_n$ del árbol de fórmulas D tal que A es A_i y B es A_j, donde $j > i$.

En el cálculo de predicados se denomina *árbol de deducción* o, simplemente, *deducción* a todo árbol de fórmulas que satisface la siguiente *exigencia estructural*: si una fórmula de la forma $\forall x A$ se obtiene en una deducción de la fórmula A según la regla de generalización, entonces la variable x no aparece libre en las hipótesis que son superiores a la aparición considerada de la fórmula $\forall x A$.

Si una fórmula que tiene la forma $\forall x A$ se obtiene de la fórmula A según la regla de generalización, y la fórmula B es superior a la aparición considerada de $\forall x A$ y contiene apariciones libres de x, entonces se dice que la variable x *varía*

en la fórmula B. La exigencia estructural puede ser expresada de la siguiente manera: en una deducción, los parámetros de las hipótesis *no varían, permanecen fijos*.

Sean Γ una lista finita de fórmulas y A una fórmula del lenguaje Ω. Diremos que la fórmula A es *deducible* en el cálculo de predicados *de la lista de fórmulas* Γ si existe una deducción D con fórmula inferior A y toda hipótesis de la deducción D es un elemento de la lista Γ. En este caso, escribiremos $\Gamma \vdash A$. Por supuesto, algunas fórmulas de Γ pueden no ser hipótesis de D. Diremos que la deducción D de la fórmula A *no depende* de estos elementos de Γ.

La lista Γ puede ser una lista vacía. En este caso, la notación $\Gamma \vdash A$ significa que existe una deducción de A sin hipótesis; escribiremos $\vdash A$ y diremos que la fórmula A es *deducible* en el cálculo de predicados.

La propia figura $\Gamma \vdash A$ es denominada a veces *argumentación*, o bien *secuencia*. De esta manera, para comprobar la secuencia $\Gamma \vdash A$, se debe construir una deducción en el cálculo de predicados con fórmula inferior A de modo que todas las hipótesis de esta deducción se encuentren en la lista Γ.

Teorema de deducción. *Si* $\Gamma, A \vdash B$, *entonces* $\Gamma \vdash \supset B$.

Si $\vdash A$, entonces A es una ley lógica. De esta manera, el cálculo de predicados puede ser considerado como cierto mecanismo formal para la obtención de leyes lógicas.

Para la deducción de fórmulas en el cálculo de predicados se utiliza un sistema de reglas derivadas elegidas especialmente denominado *técnica de deducción natural*. El lector puede ver estas reglas en [11] o, por ejemplo, en [9]. Supondremos que el lector

es capaz de deducir fórmulas en el cálculo de predicados y, a veces, omitiremos la demostración de que una u otra fórmula es deducible. A los principiantes les proponemos en estos casos al menos comprobar que estas fórmulas son leyes lógicas.

Una *teoría axiomática formal* T está definida por dos objetos: un lenguaje lógico-matemático Ω y un conjunto Y de sentencias de este lenguaje. El lenguaje Ω se denomina *lenguaje* de la teoría T, y los elementos del conjunto Y se llaman *axiomas no lógicos* de T. Señalemos que todos los axiomas no lógicos son sentencias, es decir, fórmulas cerradas del lenguaje Ω.

Diremos que una fórmula A del lenguaje Ω es *deducible en la teoría* T (en este caso, escribiremos $T \vdash A$) si existe una lista finita Γ de elementos de Y tal que $\Gamma \vdash A$ en el cálculo de predicados.

Una interpretación M del lenguaje Ω se denomina *modelo de la teoría* T si $M \models A$ para toda sentencia $A \in Y$, es decir, si todo axioma no lógico de la teoría T es verdadero en M. Si M es un modelo de la teoría T y $T \vdash B$ (donde B es una sentencia), entonces $M \models B$. De esta manera, una sentencia deducible en T es verdadera en todo modelo de la teoría T.

Describamos brevemente algunas teorías axiomáticas formales.

Aritmética elemental Ar. El lenguaje de esta teoría contiene un tipo de variables, $x, y, z, \ldots$; una constante 0; un símbolo de función monádico, Sx; y dos símbolos de función binarios, $x+y$, $x \cdot y$. Las fórmulas atómicas de Ar tienen la forma $(t = r)$, donde t, r son términos arbitrarios del lenguaje.

Los axiomas no lógicos de Ar se dividen en tres grupos: axiomas de igualdad, axiomas de Peano, axiomas que definen

la adición y la multiplicación. Posteriormente, al formular los axiomas no lógicos omitiremos los cuantificadores existenciales delante de las fórmulas. Se supone, por supuesto, que todo axioma es una proposición.

Axiomas de igualdad

1) $x = x$;
2) $x = y \wedge x = z \supset y = z$.

Axiomas de Peano:

3) $Sx \neq 0$;
4) $(Sx = Sy) \equiv x = y$;
5) $A(0) \wedge \forall x(A(x) \supset A(Sx)) \supset \forall x A(x)$ (principio de inducción completa).

Axiomas que definen la adición y la multiplicación:

6) $x + 0 = x$;
7) $x + Sy = S(x + y)$;
8) $x \cdot 0 = 0$;
9) $x \cdot Sy = x \cdot y + x$.

La axiomática de la teoría Ar se ha elegido de tal manera que todas las afirmaciones habituales que se expresan en el lenguaje de la teoría sean deducibles en ella. El modelo estándar de la teoría Ar es el modelo ω. En este modelo, las variables se consideran como variables que recorren el conjunto de los números naturales; también denotaremos este conjunto con ω, la constante representa el número natural cero, los símbolos de función se interpretan de manera evidente. Como veremos más adelante, existen otros modelos de la teoría Ar que no son isomorfos a ω. La teoría Ar es incompleta: se puede hallar una

proposición verdadera en el modelo ω, pero no deducible en Ar; esto será demostrado en la sección 3.1.

Aritmética de segundo orden Ar2. El lenguaje de esta teoría contiene dos tipos de variables. Las variables $x, y, z, \ldots$ se consideran variables que recorren el conjunto de los números naturales, las variables $X, Y, Z, \ldots$ denotan subconjuntos arbitrarios del conjunto de los números naturales. Las constantes y los símbolos de función de Ar2 son los mismos que en el lenguaje Ar. De esta manera, el lenguaje Ar2 contiene términos de dos tipos: términos para los números naturales y términos para los conjuntos de números naturales; además, los términos para los conjuntos de números naturales son sólo las variables $X, Y, Z, \ldots$. Las fórmulas atómicas de Ar2 tienen una de las dos formas siguientes: igualdades formales $(t = r)$, donde t y r son términos para los números naturales, y $(t \in X)$, donde t es un término para los números naturales y X es una variable para los conjuntos de números naturales. Las fórmulas complicadas se construyen de manera habitual, con ayuda de conectivas lógicas y cuantificadores, siendo necesario destacar que los cuantificadores se refieren a ambos tipos de variables.

Los axiomas no lógicos de Ar2 tienen la misma forma que los axiomas de Ar, con la única diferencia de que en el esquema de inducción 5 como fórmula $A(x)$ se puede tomar cualquier fórmula del lenguaje Ar2. Además, se agrega un nuevo esquema de axiomas, el *axioma de abstracción*:

10) $\exists X \forall x(x \in X \equiv A(x))$,

donde $A(x)$ es cualquier fórmula de Ar2 que no contiene apariciones libres de la variable X.

El modelo estándar de Ar2 será denotado con ω, al igual que en el caso de Ar. En este modelo, las variables $x, y, z, \ldots$ recorren el conjunto ω de todos los números naturales, y las variables $X, Y, Z, \ldots$ recorren el conjunto $P\omega$ de todos los subconjuntos de números naturales. Esta teoría tiene también muchos otros modelos interesantes que no son isomorfos a ω.

El cálculo de predicados en el lenguaje Ω también puede ser considerado como una teoría axiomática formal en el lenguaje Ω con un conjunto vacío de axiomas no lógicos. Toda interpretación del lenguaje Ω es un modelo de esta teoría.

El *cálculo de predicados puro* es, por definición, un cálculo de predicados en un lenguaje especial con un tipo de variables, sin constantes y símbolos de función, con un conjunto numerable de símbolos de predicado para cada aridad.

CAPÍTULO

1

TEORÍA DE CONJUNTOS

1.1. Lenguaje de la teoría ingenua de conjuntos. Paradojas de la teoría ingenua de conjuntos 29
1.2. Lenguaje de la teoría de conjuntos de Zermelo—Fraenkel 45
1.3. Relaciones y función en el lenguaje de la teoría de conjuntos 51
1.4. Los números naturales en la teoría de conjuntos. Escritura de las afirmaciones matemáticas en el lenguaje de la teoría de conjuntos 66
1.5. Sobre la hipótesis del continuo y el axioma de elección . . . 80
1.6. Teoría axiomática de conjuntos de Zermelo—Fraenkel . . . 85

1.1

Lenguaje de la teoría ingenua de conjuntos. Paradojas de la teoría ingenua de conjuntos

1.1.1 Pasemos ahora al estudio de un lenguaje concreto M^+ destinado a la descripción de las propiedades de los conjuntos. Nosotros partimos de la hipótesis de que existe cierta estructura matemática: una familia de conjuntos. Para cualesquiera conjuntos a y b, está determinado cuándo $a \in b$ (a pertenece a b), y cuándo esto no es cierto. Más tarde discutiremos las propiedades de la estructura $\langle M, \in \rangle$ y en qué medida es legítimo su estudio.

El lenguaje M^+ contiene un tipo de variables, $x, y, z, \ldots$, las cuales se consideran variables que denotan *conjuntos*, es decir, elementos de la estructura $\langle M, \in \rangle$.

Los conceptos de *fórmula* y *término* del lenguaje M^+ se definen al mismo tiempo e inductivamente. El punto 1 es la base de la definición, y 2–5 son los pasos inductivos:

1) Toda variable es un término.

2) Si t y r son términos, entonces $(t \in r)$ es una fórmula.

3) Si φ y ψ son fórmulas, entonces

$$(\varphi \wedge \psi),\ (\varphi \vee \psi),\ (\varphi \supset \psi),\ \neg\varphi$$

también son fórmulas.

4) Si x es una variable y φ es una fórmula, entonces $\forall x\varphi$ y $\exists x\varphi$ también son fórmulas.
5) Si x es una variable, φ es una fórmula, entonces $\{x \mid \varphi\}$ es un término.

Aquí concluye la definición.
Una fórmula de M^+ puede ser, por ejemplo,

$$\{x \mid x \in y \supset x \in z\} \in \{y \mid \neg y \in y\}.$$

El término $\{x \mid \varphi\}$ se lee así: «el conjunto de todos los x para los cuales $\varphi(x)$». Diremos que este término define el conjunto por *abstracción*, y el propio término será denominado *abstracción* respecto a la fórmula φ. La fórmula φ puede ser cualquier fórmula del lenguaje. Se dice que en el lenguaje M^+ se tiene *abstracción ilimitada.*

Señalemos que el lenguaje M^+ no es un lenguaje de primer orden precisamente debido al punto 5 de la definición, que permite definir nuevos términos a partir de fórmulas. Este efecto no existe en los lenguajes de primer orden, donde los términos se definen por separado. Se debe tener en cuenta que en el término $\{x \mid \varphi\}$ la variable x es ligada, es decir, $\{x \mid\}$ desempeña el papel de cuantificador. En el lenguaje M^+ los términos pueden contener variables ligadas, de modo que el renombramiento de variables ligadas, las colisiones de variables, etcétera, deberán referirse ahora también a los términos.

1.1.2 Introduzcamos las siguientes notaciones abreviadas:

x está incluido en y: $x \subseteq y \leftrightharpoons \forall z(z \in x \supset z \in y)$;

x es igual a y: $x = y \leftrightharpoons (x \subseteq y) \wedge (y \subseteq x)$;

x no es igual a y: $x \neq y \leftrightharpoons \neg(x = y)$;

x no pertenece a y: $x \notin y \leftrightharpoons \neg(x \in y)$;

x está incluido estrictamente en y: $x \subset y \leftrightharpoons (x \subseteq y) \vee (x \neq y)$.

Por supuesto, estas notaciones pueden ser utilizadas no solamente para las variables x e y, sino también para otros términos. En este caso, $(t \subseteq r)$ se debe obviamente interpretar como $(x \subseteq y)(x, y \,||\, t, r)$. Esta misma observación se refiere a las notaciones subsiguientes.

Utilizando las leyes de la lógica, se pueden demostrar algunos hechos que tienen lugar en $\mathfrak{M}$. Por ejemplo, en $\mathfrak{M}$ para cualquier valoración se cumple $x \subseteq x$, es decir, $x \subseteq x$ es una ley de la *teoría de conjuntos*. En efecto, $x \subseteq x$ tiene la forma $\forall z(z \in x \supset z \in x)$, lo que se deduce de la ley lógica de identidad $z \in x \supset z \in x$.

Escribiremos

$$\mathfrak{M} \cdot x \subseteq x,$$

donde el punto a la izquierda sustituye la frase «la siguiente fórmula es una ley de la teoría de conjuntos», es decir, es verdadera en $\mathfrak{M}$ para toda valoración de las variables libres.

Ejercicio. Demostrar

$$\mathfrak{M} \cdot x = x;$$

$$\mathfrak{M} \cdot x = y \supset y = x;$$

$$\mathfrak{M} \cdot x = y \wedge y = z \supset x = z.$$

1.1.3 Puesto que la estructura $\mathcal{M}$ debe reflejar las propiedades intuitivas de los conjuntos, consideramos que son leyes los siguientes dos tipos de fórmulas.

1) Axioma de extensionalidad:

$$.x = y \wedge x \in z \supset y \in z.$$

2) Axioma de abstracción:

$$.z \in \{y \mid \varphi(y)\} \equiv \varphi(z).$$

Aquí, $\varphi(z)$ es, por supuesto, $\varphi(y \parallel z)$.

Una consecuencia del axioma de extensionalidad es que la igualdad $x = y$, definida por nosotros, posee realmente las propiedades de la igualdad. Concretamente, se cumplen las *propiedades de sustitución de igual por igual*:

$$.x = y \supset (\varphi(x) \equiv \varphi(y));$$
$$.x = y \supset (t(x) = t(y)).$$

Estas dos leyes se demuestran sin dificultad a partir del axioma de extensionalidad, por inducción según la definición dada en la subsección 1.1.1, pero aquí no nos detendremos en esto y simplemente utilizaremos estas dos leyes en lo sucesivo.

El axioma de abstracción describe las propiedades de la expresión $\{x \mid \varphi\}$.

1.1.4 Introduzcamos el concepto de *par no ordenado*:

$$\{x, y\} \leftrightharpoons \{z \mid z = x \vee z = y\}.$$

Las propiedades fundamentales de esta expresión son:

1) $.u \in \{x, y\} \equiv (u = x \vee u = y)$;
2) $.x \in \{x, y\}$;
3) $.y \in \{x, y\}$;
4) $.\{x, y\} = \{y, x\}$.

► La propiedad 1 se deduce del axioma de abstracción. Demostremos la propiedad 2.

De la primera afirmación se deduce, en particular, que

$$.x \in \{x, y\} \equiv (x = x \vee x = y),$$

pero

$$.x = x \vee x = y,$$

ya que $.x = x$ (véase la subsección 1.1.2). Por consiguiente, es válido el segundo miembro de la equivalencia y, por tanto, también el primero.

Demostremos la afirmación 4. Es necesario demostrar que para todo z,

$$z \in \{x, y\} \equiv z \in \{y, x\}.$$

En virtud de la primera propiedad,

$$z \in \{x, y\} \equiv (z = x \vee z = y),$$

$$z \in \{y, x\} \equiv (z = y \vee z = x),$$

y los segundos miembros son lógicamente equivalentes. ◄

1.1.5 Llamaremos *conjunto unitario*, o bien *singletón* a todo conjunto de la forma

$$\{x\} \leftrightharpoons \{z \mid z = x\}.$$

Propiedades fundamentales:

1) $.u \in \{x\} \equiv (u = x)$; 2) $.x \in \{x\}$.

Proponemos al lector demostrar estas propiedades a manera de ejercicios.

Lema.

1) $.\{x\} = \{y\} \equiv (x = y)$;
2) $.\{x, y\} = \{u, v\} \equiv ((x = u \wedge y = v) \vee (x = v \wedge y = u))$;
3) $.\{x, y\} = \{u\} \equiv (x = u \wedge y = u)$.

▶ Demostremos 2. La implicación de derecha a izquierda se deduce simplemente de las leyes generales de la igualdad indicadas en la subsección 1.1.3. Supongamos ahora que $\{x, y\} = \{u, v\}$. Según la definición de igualdad, esto significa que

$$\forall z(z \in \{x, y\} \equiv z \in \{u, v\}).$$

Tenemos $x \in \{x, y\}$ y, por tanto, $x \in \{u, v\}$. De aquí, $x = u \vee x = v$ (véase la subsección 1.1.4). Analicemos cada caso y demostremos que en cada uno de ellos es válido

$$(x = u \wedge y = v) \vee (y = u \wedge x = v).$$

1) Supongamos que $x = u$. En virtud de $v \in \{u, v\}$, obtenemos $v \in \{x, y\}$, es decir, $v = x \vee v = y$. Si $v = y$, entonces $(x = u \wedge y = v)$, que es lo que necesitábamos. Si $v = x$, entonces en virtud de que $x = u$ tenemos $u = v$. Luego, $y \in \{x, y\}$ y, por tanto, $y \in \{u, v\}$, es decir, $y = u \vee y = v$. En virtud de $u = v$, siempre $y = v$. De esta manera, nuevamente obtenemos $(x = u \wedge y = v)$.

2) Supongamos que $x = v$. Este caso se analiza simétricamente. ◀

1.1.6 Concepto de *conjunto vacío*:

$$\varnothing \leftrightharpoons \{x \mid x \neq x\}.$$

Propiedades fundamentales:

1) $.\forall z(z \notin \varnothing)$;
2) $.\varnothing \neq \{\varnothing\}$;
3) $.\{\varnothing\} \neq \{\varnothing, \{\varnothing\}\}$.

► 1) $z \in \varnothing \equiv (z \neq z)$, pero el segundo miembro es falso (véase la subsección 1.1.2). Por tanto, $z \notin \varnothing$.

2) Tenemos $\varnothing \notin \varnothing$ y $\varnothing \in \{\varnothing\}$, por tanto,

$$\neg\forall z(z \in \varnothing \equiv z \in \{\varnothing\}),$$

es decir, $\varnothing \neq \{\varnothing\}$. ◄

Ejercicio. Demostrar $.\varnothing \subseteq u$ y, en particular, $\varnothing \subseteq \varnothing$.

Hallar ejemplos de conjuntos concretos A, B, C, D (describir los conjuntos mediante términos cerrados de M^+) tales que

$$A \subseteq B, \quad \text{pero} \quad A \notin B \quad \text{y} \quad C \in D, \quad \neg(C \subseteq D).$$

1.1.7 *Intersección, unión* y *diferencia* de dos conjuntos:

$$x \cap y \leftrightharpoons \{z \mid z \in x \wedge z \in y\};$$
$$x \cup y \leftrightharpoons \{z \mid z \in x \vee z \in y\};$$
$$x \setminus y \leftrightharpoons \{z \mid z \in x \wedge z \notin y\}.$$

1) $.u \in x \cap y \equiv (u \in x \wedge u \in y)$;
2) $.u \in x \cup y \equiv (u \in x \vee u \in y)$;
3) $.u \in x \setminus y \equiv (u \in x \wedge u \notin y)$.

▶ Estas afirmaciones se deducen directamente del axioma de abstracción. ◀

Ejercicio. Demostrar:

1) $.z \setminus (x \cap y) = (z \setminus x) \cup (z \setminus y)$;
2) $.(x \cup y) \cap z = (x \cap z) \cup (y \cap z)$.

1.1.8 Definamos ahora la *unión* y la *intersección*:

$$\cup x \leftrightharpoons \{z \mid \exists u(u \in x \wedge z \in u)\};$$

$$\cap x \leftrightharpoons \{z \mid \forall u(u \in x \supset z \in u)\}.$$

Para formular las propiedades de estos términos, introduciremos la definición general de *cuantificadores limitados*:

$$(\forall x \in y)\varphi(x) \leftrightharpoons \forall x(x \in y \supset \varphi(x));$$

$$(\exists x \in y)\varphi(x) \leftrightharpoons \exists x(x \in y \wedge \varphi(x)).$$

El primero se lee «para todo x perteneciente a y, se cumple $\varphi(x)$», y el segundo «existe un x perteneciente a y tal que se cumple $\varphi(x)$».

Nótese que para el cuantificador universal se utiliza la implicación, y para el cuantificador existencial, la conjunción. De esta manera las leyes de De Morgan son válidas también para los cuantificadores limitados.

Más exactamente,

$$.\neg(\forall x \in y)\varphi(x) \equiv (\exists x \in y)\neg\varphi(x);$$

$$.\neg(\exists x \in y)\varphi(x) \equiv (\forall x \in y)\neg\varphi(x).$$

En efecto, $\neg(\forall x \in y)\varphi(x)$ significa que $\neg\forall x(x \in y \supset \varphi(x))$ y, de acuerdo con las leyes lógicas, es equivalente a $\exists x\neg(x \in \in y \supset \varphi(x))$, y $\exists x(x \in y \wedge \neg\varphi(x))$.

De manera similar se puede definir

$$(\forall x \subseteq y)\varphi(x) \leftrightharpoons \forall (x \subseteq y \supset \varphi(x));$$
$$(\exists x \subseteq y)\varphi(x) \leftrightharpoons \exists (x \subseteq y \wedge \varphi(x)),$$

con el cumplimiento de las leyes

$$.\neg(\forall x \subseteq y)\varphi(x) \equiv (\exists x \subseteq y)\neg\varphi(x);$$
$$.\neg(\exists x \subseteq y)\varphi(x) \equiv (\forall x \subseteq y)\neg\varphi(x).$$

En el lenguaje de la aritmética se puede definir

$$(\forall x \leqslant y)A(x) \leftrightharpoons \forall x(x \leqslant y \supset A(x));$$
$$(\exists x \leqslant y)A(x) \leftrightharpoons \exists x(x \leqslant y \wedge A(x)).$$

Nuevamente tendremos, por ejemplo,

$$\omega \models \neg(\exists x \leqslant y)A(x) \equiv (\forall x \leqslant y)\neg A(x).$$

Nótese que el signo de desigualdad en las leyes de De Morgan «no se invierte». A veces, el estudiante tiende a afirmar erróneamente que

$$\omega \models \neg(\exists x \leqslant y)A(x) \equiv (\forall x > y)\neg A(x).$$

Las propiedades fundamentales de la unión y la intersección son

1) $.z \in \cup x \equiv (\exists u \in x)(z \in u)$;
2) $.z \in \cap x \equiv (\forall u \in x)(z \in u)$.

► Estas propiedades se cumplen en virtud del axioma de abstracción y la definición. ◄

1.1.9 El *conjunto universal* (*universo, conjunto de todos los conjuntos*) se define de la siguiente manera:

$$V = \{z \mid z = z\}.$$

Por tanto, $.\forall\, z(z \in V)$.

► Por definición, $z \in V \equiv (z = z)$, y el segundo miembro de esta equivalencia es válido (véase la subsección 1.1.2). ◄

El *complemento general* se define de la siguiente manera:

$$\bar{x} \leftrightharpoons V \setminus x.$$

Ejercicio.

$$.\overline{x \cup y} = \bar{x} \cap \bar{y}; \quad .x \setminus y = x \cap \bar{y}.$$

Lema.

$$.\cup \varnothing = \varnothing; \quad .\cap \varnothing = V.$$

► Demostremos la primera ley. Tenemos

$$z \in \cup\varnothing \equiv (\exists\, u \in \varnothing)(z \in u),$$

y el segundo miembro de esta equivalencia es falso, ya que $\forall\, u(u \notin \varnothing)$. Por consiguiente, $z \notin \cup\varnothing$ para todo z y, por tanto, $\cup\varnothing = \varnothing$. Demostremos ahora la segunda ley. Tenemos $z \in \cap\varnothing \equiv (\forall\, u \in \varnothing)(z \in u)$, y el segundo miembro de esta equivalencia es verdadero (en virtud de la falsedad de la premisa de la implicación). Por consiguiente, $z \in \cap\varnothing$ para todo z y, por tanto, $\cap\varnothing = V$. ◄

1.1.10 El *conjunto de todos los subconjuntos* (*conjunto potencia*) se define de la siguiente manera:

$$Px \leftrightharpoons \{z \mid z \subseteq x\}; \quad .u \in Px \equiv (u \subseteq x).$$

1.1.11 Demos la definición de un conjunto infinito estándar. Introduzcamos la operación teórico-conjuntista de *sucesión*:

$$Sx \leftrightharpoons x \cup \{x\}.$$

Un conjunto x se denomina *conjunto progresivo* si él contiene $\varnothing$ y es cerrado respecto a la operación S. Expresemos esta definición mediante fórmulas:

$$\mathrm{Prog}(x) \leftrightharpoons (\varnothing \in x) \wedge \forall z(z \in x \supset Sz \in x).$$

Como conjunto infinito estándar tomemos la intersección de la familia formada por todos los conjuntos progresivos:

$$\omega \leftrightharpoons \cap\{x \mid \mathrm{Prog}(x)\}.$$

Intuitivamente, es obvio que ω está formado por la siguiente sucesión de elementos:

$$\varnothing, \quad \{\varnothing\}, \quad \{\varnothing, \{\varnothing\}\}, \quad \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \quad \ldots .$$

Cada elemento de esta sucesión se obtiene del elemento anterior mediante la operación S. Todos los elementos son diferentes, de modo que ω es infinito. El n-ésimo elemento de la sucesión (si se cuenta desde cero) es un conjunto de n elementos. Estas ideas intuitivas se pueden expresar exactamente:

1) $.\varnothing \in \omega$;
2) $.z \in \omega \supset Sz \in \omega$;
3) $.\mathrm{Prog}(x) \supset (\omega \subseteq x)$.

► Por definición, $u \in \omega \equiv \forall x(\mathrm{Prog}(x) \supset u \in x)$. Si aquí, en lugar de u, escribimos $\varnothing$, entonces el segundo miembro de esta

equivalencia es válido (en virtud de la definición de Prog(x)). Por consiguiente, $\varnothing \in \omega$. Demostremos 2. Si $z \in \omega$, entonces $z \in x$ para todo x, Prog(x). Pero entonces también $Sz \in x$ para todo x, Prog(x), es decir, $Sz \in \omega$. Finalmente, demostremos 3. Supongamos que Prog(x). Es necesario demostrar $\omega \subseteq x$, es decir, $z \in \omega \supset z \in x$ para todo z. Pero si $z \in \omega$ entonces, por supuesto, $z \in x$ en virtud de Prog(x). ◀

1.1.12 Introduzcamos ahora dos notaciones especiales para algunos términos del tipo de abstracción.

Definición de un conjunto por comprehensión:

$$\{x \in y \mid \varphi(x)\} \leftrightharpoons \{x \mid x \in y \wedge \varphi(x)\}.$$

La expresión de la izquierda se lee como «el conjunto de todos los x pertenecientes a y tales que $\varphi(x)$». En este caso, la variable x es ligada y la variable y es libre. Aquí suponemos que x es diferente de y. En general, la variable y se puede sustituir, por supuesto correctamente, por los términos (renombrando la variable ligada x si es necesario).

La propiedad fundamental de esta notación es la siguiente:

$$.u \in \{x \in y \mid \varphi(x)\} \equiv (u \in y \wedge \varphi(u)).$$

Definición de un conjunto por reemplazo:

$$\{y \mid x \in u,\ (x \mapsto y),\ \varphi(x, y)\} \leftrightharpoons$$
$$\leftrightharpoons \{y \mid (\exists\, x \in u)(\varphi(x, y) \wedge \forall\, z(\varphi(x, z) \supset y = z))\}.$$

Aquí, x, y, u son variables diferentes; además, x e y son ligadas, y u es libre.

De esta manera, a la izquierda tenemos la notación de un conjunto Q tal que $y \in Q \Leftrightarrow$ existe un $x \in u$ tal que para x es válido $\varphi(x, y)$, y el y indicado es *único*. En otras palabras, consideraremos diferentes $x \in u$. Para algunos $x \in u$ no existe un y tal que $\varphi(x, y)$. Para algunos $x \in u$ existen muchos y tales que $\varphi(x, y)$. Finalmente, para algunos $x \in u$ existe exactamente un y tal que $\varphi(x, y)$. Todos estos y serán incluidos en el conjunto Q.

Estas ideas intuitivas pueden ser expresadas como afirmaciones exactas.

Supongamos a continuación que Q denota el término

$$\{y \mid x \in u,\ (x \mapsto y),\ \varphi(x, y)\},$$

$$.z \in Q \equiv (\exists\, x \in u)(\varphi(x, z) \wedge \forall\, v(\varphi(x, v) \supset z = v)).$$

► La afirmación se deduce directamente de la definición. ◄

Introduzcamos la siguiente abreviación (se lee «existe uno y sólo un x tal que $\varphi(x)$»):

$$\exists! x\, \varphi(x) \leftrightharpoons \exists\, x\, \varphi(x) \wedge \forall\, y\, z(\varphi(y) \wedge \varphi(z) \supset y = z).$$

Ejercicio. $x \in u \wedge \exists! v\, \varphi(x, v) \wedge \varphi(x, y) \supset y \in Q$.

1.1.13 Consideremos el *conjunto de Russell*

$$R \leftrightharpoons \{x \mid x \notin x\}.$$

Éste es un conjunto concreto descrito por un término cerrado del lenguaje M^+.

Según el axioma de abstracción, para todo u tenemos

$$.u \in R \equiv u \notin u.$$

En particular, si sustituimos u por el conjunto R, obtenemos

$$.R \in R \equiv R \notin R.$$

Por otra parte, es evidente que $\neg(R \in R \equiv R \notin R)$.

Hemos obtenido una contradicción.

Este breve razonamiento es lo que se denomina *paradoja de Russell* en el lenguaje M^+.

Discutamos brevemente la naturaleza de las paradojas del tipo de la paradoja de Russell.

Consideremos el siguiente enunciado:

«La proposición escrita en este renglón es falsa».

¿Es verdadera o falsa la proposición escrita entre comillas? Partiendo de su sentido se puede concluir que ella es verdadera si y sólo si ella es falsa, lo que evidentemente es una contradicción. La causa de esta paradoja se puede atribuir a la estructura de la proposición escrita entre comillas; ella se refiere a sí misma. Aquí se manifiesta la *abstracción de enajenación*, en virtud de la cual el investigador convierte el proceso de su investigación, sus razonamientos, en objeto de la investigación. Como vemos, si esto se realiza sin cuidado, se obtienen enunciados internamente contradictorios.

En una forma algo diferente, esta paradoja es conocida como la *paradoja de Eubúlides* (siglo IV a. C.), o *paradoja del mentiroso*. Supongamos que alguien dice: «Yo miento». ¿Es verdadera o falsa esta proposición?

Por supuesto, las paradojas se pueden evitar si consideramos las proposiciones indicadas carentes de sentido (o incorrectamente formadas). Pero en este caso surge un problema difícil: ¿qué

proposiciones tienen sentido? ¿No resultará que afirmaciones de la matemática o la física que parecían confiables son internamente contradictorias? ¿Cuáles son los criterios que diferencian las proposiciones con sentido de las proposiciones sin sentido?

Un análisis cuidadoso muestra que en la teoría de conjuntos surge una situación análoga cuando se utiliza el axioma de abstracción (véase la subsección 1.1.3). Primeramente, el investigador formula la propiedad $\varphi(y)$ y, a continuación, forma el objeto de investigación, el conjunto $\{y \mid \varphi(y)\}$. La propiedad $\varphi(y)$ puede expresar algo sobre todos los conjuntos, incluido el nuevo conjunto $\{y \mid \varphi(y)\}$. De este modo, tiene lugar una referencia a sí mismo. Por ejemplo, $\varphi(y)$ puede contener cuantificadores que se refieren a variables que, naturalmente, se toman como variables que representan cualesquiera conjuntos, incluido el conjunto $\{y \mid \varphi(y)\}$. En cierto sentido, el conjunto $\{y \mid \varphi(y)\}$ no se puede considerar como recientemente formado, puesto que de él ya se habla en la formulación de la propiedad $\varphi(y)$. Éste fenómeno se denomina *impredicatividad de la teoría de conjuntos.*

La renuncia total a las *definiciones impredicativas* exige una considerable reestructuración de la matemática existente, por lo que habitualmente se adopta una postura de compromiso. En los casos necesarios, se utiliza el principio impredicativo de abstracción, pero se aplica de manera limitada para evitar el surgimiento de paradojas.

Analicemos ahora otra situación paradójica. El barbero de una pequeña villa afeita sólo a aquellas personas de la villa que no se afeitan a sí mismas. ¿Se afeita el barbero a sí mismo? Un simple razonamiento muestra que él se afeita cuando, y sólo cuando, él no se afeita a sí mismo.

¿Cómo debemos reaccionar ante esta situación? Es muy sencillo. Simplemente, este barbero no existe. La condición a la que debe someterse este barbero hipotético es internamente contradictoria, es imposible cumplirla (aunque esto no se nota inmediatamente). Por supuesto, esto no elimina todos los problemas que origina este sutil ejemplo. En este caso, la pregunta más importante es cómo determinar qué condiciones son internamente contradictorias y cuáles no. ¿Será posible indicar con toda seguridad una clase de condiciones que a ciencia cierta no son contradictorias.

Es natural considerar de la misma manera que el conjunto R no existe. Sin embargo, en este caso sería necesario someter a revisión las concepciones que tenemos acerca de la estructura $\mathcal{M}$ de la teoría de conjuntos y cambiar la estructura del lenguaje M^+. Hasta ahora suponíamos que *todo término cerrado de* M^+ *definía un conjunto*, es decir, considerábamos que cualquier condición $\varphi(x)$ definía un objeto $\{x \mid \varphi(x)\}$. Sin embargo, como hemos visto, este punto de vista es contradictorio por sí mismo. Es necesario indicar una clase de condiciones que de antemano definen conjuntos, y el número de estos conjuntos debe ser suficiente para satisfacer las necesidades matemáticas habituales. Al mismo tiempo, se debe reconocer que algunas condiciones no definen conjuntos.

La lógica matemática moderna está aún muy lejana de la solución completa de este problema. Existen varias soluciones cómodas desde el punto de vista práctico. La más popular de ellas es, por lo visto, la propuesta por Zermelo y perfeccionada por Fraenkel. La idea principal radica en que renunciamos a los conjuntos «demasiado grandes», de potencia indeterminada, como, por ejemplo, el conjunto universal.

1.2 Lenguaje de la teoría de conjuntos de Zermelo—Fraenkel

1.2.1 Nuevamente partimos de la hipótesis de que existe una estructura matemática $\mathcal{U}_0$, a saber, una familia de conjuntos con la relación $a \in b$. Sus propiedades están definidas por *convenios semánticos* que vamos a denominar (de una manera algo imprecisa) *axiomas de la teoría de conjuntos de Zermelo—Fraenkel.*

El lenguaje ZF^+ contiene un tipo de variables, $x, y, z, \ldots$, que se consideran variables que denotan conjuntos.

Los conceptos de *fórmula* y *término* de ZF^+ se definen por inducción simultánea:

1) Una variable es un término.
2) Si t y r son términos, entonces $(t \in r)$ es una fórmula.
3) Si φ y ψ son fórmulas, entonces

$$(\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \supset \psi), \quad \neg\varphi$$

también son fórmulas.

4) Si x es una variable y φ es una fórmula, entonces $\forall x\varphi$ y $\exists x\varphi$ son fórmulas.

5) Los símbolos $\varnothing$ y ω son términos.
6) Si t y r son términos, entonces $\{t, r\}$ es un término.
7) Si t es un término, entonces Pt y $\cup t$ son términos.
8) Si φ es una fórmula y t es un término que no contiene apariciones libres de la variable x, entonces $\{x \in t \mid \varphi\}$ es un término.
9) Si φ es una fórmula, x, y son variables diferentes, y t es un término que no contiene apariciones libres de las variables x e y, entonces

$$\{y \mid x \in t,\ (x \mapsto y),\ \varphi\}$$

es un término.

Ésta es la definición de fórmula y término.

La idea del lenguaje ZF^+ consiste en que en él se incluye sólo una parte de las construcciones de M^+, con lo que se evitan las paradojas conocidas. Ahora $\varnothing$, ω, $\cup$, P no se definen, sino que son símbolos independientes. En lugar del axioma de abstracción ilimitada, sólo tenemos sus casos particulares, incluidas la definición por comprehensión y la definición por reemplazo.

1.2.2 Consideraremos que las siguientes fórmulas son leyes de la estructura $\mathcal{M}_0$:

1) Axioma de extensionalidad:

$$.x = y \wedge x \in z \supset y \in z.$$

Para nosotros es esencial que a partir de este axioma (con ayuda de los demás axiomas) se deducen las propiedades

de la igualdad:

$$.x = y \supset (\varphi(x) \equiv \varphi(y)); \quad .x = y \supset (t(x) = t(y))$$

(compárese con la subsección 1.1.3). Aquí, $x \subseteq y$ y $x = y$ se definen como antes (véase la subsección 1.1.2).

2) Axioma del conjunto vacío:

$$.\forall z(z \notin \varnothing).$$

En M^+ esta propiedad se demuestra, y el símbolo $\varnothing$ se define de manera especial. En el lenguaje ZF^+, el símbolo $\varnothing$ es independiente, y sus propiedades deben ser definidas. Esta observación se refiere también a las otras construcciones de ZF^+.

3) Axioma del par no ordenado:

$$.\forall z(z \in \{x, y\} \equiv (z = x \vee z = y)).$$

Las propiedades del par no ordenado que vimos en las subsecciones 1.1.4 y 1.1.5 se pueden demostrar también en ZF^+, ya que todas ellas se deducen de la propiedad 1 de la subsección 1.1.4, y esta propiedad del par no ordenado se cumple también en ZF^+. Introduzcamos a continuación la siguiente definición: $\{x\} \leftrightharpoons \{x, x\}$. Entonces la propiedad fundamental 1 de $\{x\}$ de la subsección 1.1.5 también se cumple en ZF^+.

4) Axioma de la suma (unión):

$$.\forall z(z \in \cup x \equiv (\exists u \in x)(z \in u)).$$

Por tanto, la propiedad fundamental 1 de la unión de conjuntos de la subsección 1.1.8 se cumple también en ZF^+.

5) Axioma del conjunto potencia:

$$.\forall z(z \in Px \equiv (z \subseteq x))$$

(compárese con la subsección 1.1.10).

6) Axiomas de infinitud:

$$.\varnothing \in \omega; \quad .(\forall z \in \omega)(Sz \in \omega); \quad .\forall x(\mathrm{Prog}(x) \supset (\omega \subseteq x))$$

(compárese con la subsección 1.1.11).

7) Axioma de comprehensión:

$$.\forall z(z \in \{x \in t \mid \varphi(x)\} \equiv (z \in t \wedge \varphi(z)))$$

(compárese con la subsección 1.1.12).

8) Axioma de reemplazo:

$$.\forall z\big(z \in \{y \mid x \in u,\ (x \mapsto y),\ \varphi(x,y)\} \equiv$$
$$\equiv (\exists x \in u)(\varphi(x,z) \wedge \forall v(\varphi(x,v) \supset z = v))\big)$$

(compárese con la subsección 1.1.12).

Éstos son los *convenios semánticos* de ZF^+. Nótese que en el sentido natural ZF^+ es parte del lenguaje M^+ de la *teoría ingenua de conjuntos*.

En el lenguaje ZF^+ no existe la posibilidad de formar el conjunto universal $V = \{x \mid x = x\}$ o el *conjunto de Russell* $R = \{x \mid x \notin x\}$. Simplemente para esto no existen los medios lingüísticos adecuados. Consideramos que estos conjuntos no están presentes en la estructura $\mathcal{U}_0$.

1.2.3 Ahora debemos comprobar que los conjuntos habituales utilizados en la matemática se expresan en ZF^+. Comencemos con el análisis de las construcciones ya tratadas en la sección 1.1.

La intersección, la unión y el complemento de dos conjuntos pueden ser definidos en ZF^+:

$$x \cup y \leftrightharpoons \cup\{x, y\};$$
$$x \cap y \leftrightharpoons \{z \in (x \cup y) \mid z \in x \wedge z \in y\};$$
$$x \setminus y \leftrightharpoons \{z \in x \mid z \notin y\}.$$

Ejercicio. Demostrar que las propiedades de estos conceptos (véase la subsección 1.1.7) se cumplen también para la nueva definición.

Algo más difícil es definir la intersección de una familia de conjuntos. Es imposible definir $\cap x$ de manera que se cumpla la propiedad fundamental

$$z \in \cap x \equiv (\forall u \in x)(z \in u),$$

de la subsección 1.1.8. Si esto fuera posible, entonces, de acuerdo con el lema de la subsección 1.1.9, tendríamos $\cap\varnothing = V$. Sin embargo, en ZF^+ se puede definir un concepto muy parecido:

$$\cap x \leftrightharpoons \{z \in \cup x \mid (\forall u \in x)(z \in u)\}.$$

Lema. *Se cumplen las siguientes propiedades:*

1) $x \neq \varnothing \supset \forall z(z \in \cap x \equiv (\forall u \in x)(z \in u))$;
2) $\cap\varnothing = \varnothing$.

► Si $x \neq \varnothing$, entonces existe $u_0 \in x$. En este caso, de

$$(\forall u \in x)(z \in u)$$

se deduce $z \in u_0$ y, por tanto, $z \in \cup x$, de modo que la restricción impuesta por el axioma de comprehensión no es esencial (condición ficticia). Puesto que $\cup\varnothing = \varnothing$, se cumple $\cap\varnothing = \varnothing$. ◀

Naturalmente, en ZF^+ debemos renunciar al *complemento general*, ya que en caso contrario tendríamos $\overline{\varnothing} = V$. No puede existir un conjunto V tal que $\forall z(z \in V)$, ya que de otro modo podríamos definir por comprehensión el conjunto de Russell

$$R = \{z \in V \mid z \notin z\}.$$

1.3 Relaciones y función en el lenguaje de la teoría de conjuntos

1.3.1 Un *par ordenado* (según Kuratowski) se define de la siguiente manera:

$$\langle x, y\rangle \leftrightharpoons \{\{x\},\ \{x, y\}\}.$$

La propiedad fundamental de este conjunto se expresa mediante el siguiente lema.

Lema. $\langle x, y\rangle = \langle u, v\rangle \equiv (x = u \wedge y = v)$.

▶ La implicación de derecha a izquierda es consecuencia de las propiedades de la igualdad. Supongamos ahora que $\langle x, y\rangle = \langle u, v\rangle$ y demostremos que $x = u \wedge y = v$.

Según la suposición, $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. De acuerdo con la afirmación 2 del lema de la subsección 1.1.5, tenemos

$$\{x\} = \{u\} \wedge \{x, y\} = \{u, v\}$$

o bien

$$\{x\} = \{u, v\} \wedge \{x, y\} = \{u\}.$$

En particular, si sustituimos u por el conjunto R, obtenemos

$$.R \in R \equiv R \notin R.$$

Por otra parte, es evidente que $\neg(R \in R \equiv R \notin R)$.

Hemos obtenido una contradicción.

Este breve razonamiento es lo que se denomina *paradoja de Russell* en el lenguaje M^+.

Discutamos brevemente la naturaleza de las paradojas del tipo de la paradoja de Russell.

Consideremos el siguiente enunciado:

«La proposición escrita en este renglón es falsa».

¿Es verdadera o falsa la proposición escrita entre comillas? Partiendo de su sentido se puede concluir que ella es verdadera si y sólo si ella es falsa, lo que evidentemente es una contradicción. La causa de esta paradoja se puede atribuir a la estructura de la proposición escrita entre comillas; ella se refiere a sí misma. Aquí se manifiesta la *abstracción de enajenación*, en virtud de la cual el investigador convierte el proceso de su investigación, sus razonamientos, en objeto de la investigación. Como vemos, si esto se realiza sin cuidado, se obtienen enunciados internamente contradictorios.

En una forma algo diferente, esta paradoja es conocida como la *paradoja de Eubúlides* (siglo IV a. C.), o *paradoja del mentiroso*. Supongamos que alguien dice: «Yo miento». ¿Es verdadera o falsa esta proposición?

Por supuesto, las paradojas se pueden evitar si consideramos las proposiciones indicadas carentes de sentido (o incorrectamente formadas). Pero en este caso surge un problema difícil: ¿qué

proposiciones tienen sentido? ¿No resultará que afirmaciones de la matemática o la física que parecían confiables son internamente contradictorias? ¿Cuáles son los criterios que diferencian las proposiciones con sentido de las proposiciones sin sentido?

Un análisis cuidadoso muestra que en la teoría de conjuntos surge una situación análoga cuando se utiliza el axioma de abstracción (véase la subsección 1.1.3). Primeramente, el investigador formula la propiedad $\varphi(y)$ y, a continuación, forma el objeto de investigación, el conjunto $\{y \mid \varphi(y)\}$. La propiedad $\varphi(y)$ puede expresar algo sobre todos los conjuntos, incluido el nuevo conjunto $\{y \mid \varphi(y)\}$. De este modo, tiene lugar una referencia a sí mismo. Por ejemplo, $\varphi(y)$ puede contener cuantificadores que se refieren a variables que, naturalmente, se toman como variables que representan cualesquiera conjuntos, incluido el conjunto $\{y \mid \varphi(y)\}$. En cierto sentido, el conjunto $\{y \mid \varphi(y)\}$ no se puede considerar como recientemente formado, puesto que de él ya se habla en la formulación de la propiedad $\varphi(y)$. Éste fenómeno se denomina *impredicatividad de la teoría de conjuntos.*

La renuncia total a las *definiciones impredicativas* exige una considerable reestructuración de la matemática existente, por lo que habitualmente se adopta una postura de compromiso. En los casos necesarios, se utiliza el principio impredicativo de abstracción, pero se aplica de manera limitada para evitar el surgimiento de paradojas.

Analicemos ahora otra situación paradójica. El barbero de una pequeña villa afeita sólo a aquellas personas de la villa que no se afeitan a sí mismas. ¿Se afeita el barbero a sí mismo? Un simple razonamiento muestra que él se afeita cuando, y sólo cuando, él no se afeita a sí mismo.

¿Cómo debemos reaccionar ante esta situación? Es muy sencillo. Simplemente, este barbero no existe. La condición a la que debe someterse este barbero hipotético es internamente contradictoria, es imposible cumplirla (aunque esto no se nota inmediatamente). Por supuesto, esto no elimina todos los problemas que origina este sutil ejemplo. En este caso, la pregunta más importante es cómo determinar qué condiciones son internamente contradictorias y cuáles no. ¿Será posible indicar con toda seguridad una clase de condiciones que a ciencia cierta no son contradictorias.

Es natural considerar de la misma manera que el conjunto R no existe. Sin embargo, en este caso sería necesario someter a revisión las concepciones que tenemos acerca de la estructura $\mathcal{U}$ de la teoría de conjuntos y cambiar la estructura del lenguaje M^+. Hasta ahora suponíamos que *todo término cerrado de* M^+ *definía un conjunto*, es decir, considerábamos que cualquier condición $\varphi(x)$ definía un objeto $\{x \mid \varphi(x)\}$. Sin embargo, como hemos visto, este punto de vista es contradictorio por sí mismo. Es necesario indicar una clase de condiciones que de antemano definen conjuntos, y el número de estos conjuntos debe ser suficiente para satisfacer las necesidades matemáticas habituales. Al mismo tiempo, se debe reconocer que algunas condiciones no definen conjuntos.

La lógica matemática moderna está aún muy lejana de la solución completa de este problema. Existen varias soluciones cómodas desde el punto de vista práctico. La más popular de ellas es, por lo visto, la propuesta por Zermelo y perfeccionada por Fraenkel. La idea principal radica en que renunciamos a los conjuntos «demasiado grandes», de potencia indeterminada, como, por ejemplo, el conjunto universal.

1.2

Lenguaje de la teoría de conjuntos de Zermelo—Fraenkel

1.2.1 Nuevamente partimos de la hipótesis de que existe una estructura matemática $\mathcal{U}_0$, a saber, una familia de conjuntos con la relación $a \in b$. Sus propiedades están definidas por *convenios semánticos* que vamos a denominar (de una manera algo imprecisa) *axiomas de la teoría de conjuntos de Zermelo—Fraenkel.*

El lenguaje ZF^+ contiene un tipo de variables, $x, y, z, \ldots$, que se consideran variables que denotan conjuntos.

Los conceptos de *fórmula* y *término* de ZF^+ se definen por inducción simultánea:

1) Una variable es un término.
2) Si t y r son términos, entonces $(t \in r)$ es una fórmula.
3) Si φ y ψ son fórmulas, entonces

$$(\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \supset \psi), \quad \neg\varphi$$

también son fórmulas.

4) Si x es una variable y φ es una fórmula, entonces $\forall x\varphi$ y $\exists x\varphi$ son fórmulas.

5) Los símbolos $\varnothing$ y ω son términos.
6) Si t y r son términos, entonces $\{t, r\}$ es un término.
7) Si t es un término, entonces Pt y $\cup t$ son términos.
8) Si φ es una fórmula y t es un término que no contiene apariciones libres de la variable x, entonces $\{x \in t \mid \varphi\}$ es un término.
9) Si φ es una fórmula, x, y son variables diferentes, y t es un término que no contiene apariciones libres de las variables x e y, entonces

$$\{y \mid x \in t,\ (x \mapsto y),\ \varphi\}$$

es un término.

Ésta es la definición de fórmula y término.

La idea del lenguaje ZF^+ consiste en que en él se incluye sólo una parte de las construcciones de M^+, con lo que se evitan las paradojas conocidas. Ahora $\varnothing$, ω, $\cup$, P no se definen, sino que son símbolos independientes. En lugar del axioma de abstracción ilimitada, sólo tenemos sus casos particulares, incluidas la definición por comprehensión y la definición por reemplazo.

1.2.2 Consideraremos que las siguientes fórmulas son leyes de la estructura $\mathcal{M}_0$:

1) Axioma de extensionalidad:

$$.x = y \wedge x \in z \supset y \in z.$$

Para nosotros es esencial que a partir de este axioma (con ayuda de los demás axiomas) se deducen las propiedades

de la igualdad:

$$.x = y \supset (\varphi(x) \equiv \varphi(y)); \quad .x = y \supset (t(x) = t(y))$$

(compárese con la subsección 1.1.3). Aquí, $x \subseteq y$ y $x = y$ se definen como antes (véase la subsección 1.1.2).

2) Axioma del conjunto vacío:

$$.\forall z(z \notin \varnothing).$$

En M^+ esta propiedad se demuestra, y el símbolo $\varnothing$ se define de manera especial. En el lenguaje ZF^+, el símbolo $\varnothing$ es independiente, y sus propiedades deben ser definidas. Esta observación se refiere también a las otras construcciones de ZF^+.

3) Axioma del par no ordenado:

$$.\forall z(z \in \{x, y\} \equiv (z = x \vee z = y)).$$

Las propiedades del par no ordenado que vimos en las subsecciones 1.1.4 y 1.1.5 se pueden demostrar también en ZF^+, ya que todas ellas se deducen de la propiedad 1 de la subsección 1.1.4, y esta propiedad del par no ordenado se cumple también en ZF^+. Introduzcamos a continuación la siguiente definición: $\{x\} \leftrightharpoons \{x, x\}$. Entonces la propiedad fundamental 1 de $\{x\}$ de la subsección 1.1.5 también se cumple en ZF^+.

4) Axioma de la suma (unión):

$$.\forall z(z \in \cup x \equiv (\exists u \in x)(z \in u)).$$

Por tanto, la propiedad fundamental 1 de la unión de conjuntos de la subsección 1.1.8 se cumple también en ZF^+.

5) Axioma del conjunto potencia:

$$.\forall\, z(z \in Px \equiv (z \subseteq x))$$

(compárese con la subsección 1.1.10).

6) Axiomas de infinitud:

$$.\varnothing \in \omega; \quad .(\forall\, z \in \omega)(Sz \in \omega); \quad .\forall\, x(\mathrm{Prog}(x) \supset (\omega \subseteq x))$$

(compárese con la subsección 1.1.11).

7) Axioma de comprehensión:

$$.\forall\, z(z \in \{x \in t \mid \varphi(x)\} \equiv (z \in t \wedge \varphi(z)))$$

(compárese con la subsección 1.1.12).

8) Axioma de reemplazo:

$$.\forall\, z\big(z \in \{y \mid x \in u,\ (x \mapsto y),\ \varphi(x,y)\} \equiv \\ \equiv (\exists\, x \in u)(\varphi(x,z) \wedge \forall\, v(\varphi(x,v) \supset z = v))\big)$$

(compárese con la subsección 1.1.12).

Éstos son los *convenios semánticos* de ZF^+. Nótese que en el sentido natural ZF^+ es parte del lenguaje M^+ de la *teoría ingenua de conjuntos*.

En el lenguaje ZF^+ no existe la posibilidad de formar el conjunto universal $V = \{x \mid x = x\}$ o el *conjunto de Russell* $R = \{x \mid x \notin x\}$. Simplemente para esto no existen los medios lingüísticos adecuados. Consideramos que estos conjuntos no están presentes en la estructura $\mathcal{M}_0$.

1.2.3 Ahora debemos comprobar que los conjuntos habituales utilizados en la matemática se expresan en ZF^+. Comencemos con el análisis de las construcciones ya tratadas en la sección 1.1.

La intersección, la unión y el complemento de dos conjuntos pueden ser definidos en ZF^+:

$$x \cup y \leftrightharpoons \cup\{x, y\};$$
$$x \cap y \leftrightharpoons \{z \in (x \cup y) \mid z \in x \wedge z \in y\};$$
$$x \setminus y \leftrightharpoons \{z \in x \mid z \notin y\}.$$

Ejercicio. Demostrar que las propiedades de estos conceptos (véase la subsección 1.1.7) se cumplen también para la nueva definición.

Algo más difícil es definir la intersección de una familia de conjuntos. Es imposible definir $\cap x$ de manera que se cumpla la propiedad fundamental

$$z \in \cap x \equiv (\forall u \in x)(z \in u),$$

de la subsección 1.1.8. Si esto fuera posible, entonces, de acuerdo con el lema de la subsección 1.1.9, tendríamos $\cap\varnothing = V$. Sin embargo, en ZF^+ se puede definir un concepto muy parecido:

$$\cap x \leftrightharpoons \{z \in \cup x \mid (\forall u \in x)(z \in u)\}.$$

Lema. *Se cumplen las siguientes propiedades:*

1) $x \neq \varnothing \supset \forall z(z \in \cap x \equiv (\forall u \in x)(z \in u))$;
2) $\cap\varnothing = \varnothing$.

► Si $x \neq \varnothing$, entonces existe $u_0 \in x$. En este caso, de

$$(\forall u \in x)(z \in u)$$

se deduce $z \in u_0$ y, por tanto, $z \in \cup x$, de modo que la restricción impuesta por el axioma de comprehensión no es esencial (condición ficticia). Puesto que $\cup\varnothing = \varnothing$, se cumple $\cap\varnothing = \varnothing$. ◀

Naturalmente, en ZF^+ debemos renunciar al *complemento general*, ya que en caso contrario tendríamos $\overline{\varnothing} = V$. No puede existir un conjunto V tal que $\forall z(z \in V)$, ya que de otro modo podríamos definir por comprehensión el conjunto de Russell

$$R = \{z \in V \mid z \notin z\}.$$

1.3 Relaciones y función en el lenguaje de la teoría de conjuntos

1.3.1 Un *par ordenado* (según Kuratowski) se define de la siguiente manera:

$$\langle x, y\rangle \leftrightharpoons \{\{x\},\ \{x, y\}\}.$$

La propiedad fundamental de este conjunto se expresa mediante el siguiente lema.

Lema. $\langle x, y\rangle = \langle u, v\rangle \equiv (x = u \wedge y = v)$.

► La implicación de derecha a izquierda es consecuencia de las propiedades de la igualdad. Supongamos ahora que $\langle x, y\rangle = \langle u, v\rangle$ y demostremos que $x = u \wedge y = v$.

Según la suposición, $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. De acuerdo con la afirmación 2 del lema de la subsección 1.1.5, tenemos

$$\{x\} = \{u\} \wedge \{x, y\} = \{u, v\}$$

o bien

$$\{x\} = \{u, v\} \wedge \{x, y\} = \{u\}.$$

Analicemos estos dos casos.

a) $\{x\} = \{u, v\}$, $\{x, y\} = \{u\}$. En virtud de la subsección 1.1.5, tenemos $x = y = u = v$, de modo que, evidentemente, $x = u \wedge y = v$.

b) $\{x\} = \{u\}$, $\{x, y\} = \{u, v\}$. En virtud de la subsección 1.1.5, tenemos $x = u$.

Ahora tenemos dos casos:

$$x = u \wedge y = v, \quad \text{o bien} \quad x = v \wedge y = u.$$

En el primer caso, obtenemos lo que necesitamos. En el segundo, en virtud de que $x = u$, obtenemos $x = u = y = v$, es decir, nuevamente $x = u \wedge y = v$. ◀

Ahora podemos definir las *ternas ordenadas, las 4-tuplas ordenadas*, etcétera:

$$\langle x \rangle \leftrightharpoons x;$$

$$\langle x_1, \ldots, x_n, x_{n+1} \rangle \leftrightharpoons \langle \langle x_1, \ldots, x_n \rangle, x_{n+1} \rangle.$$

Del lema se deduce una afirmación más general:

$$.\langle x_1, \ldots, x_n \rangle = \langle u_1, \ldots, u_n \rangle \equiv (x_1 = u_1 \wedge \ldots \wedge x_n = u_n).$$

Señalemos que según esta definición toda *n-tupla ordenada* para $n > 0$ es al mismo tiempo un par ordenado.

1.3.2 Por definición, una *relación* es un conjunto cada elemento del cual es un par ordenado. En el lenguaje considerado, «ser una relación» se escribe de la siguiente manera:

$$\mathrm{Rel}(x) \leftrightharpoons (\forall\, z \in x)\, \exists\, uv(z = \langle u, v \rangle).$$

Diremos que u y v *se encuentran en una relación* x si $\langle u,v\rangle \in x$. A veces esto se escribe como uxv.

Se denomina *campo de una relación* x al conjunto de todos los u tales que u figura en x como elemento izquierdo de algún par o como elemento derecho de algún par.

En el lenguaje considerado, el campo de una relación puede ser definido de la siguiente manera:

$$\mathrm{Fld}(x) \leftrightharpoons \cup\cup x.$$

El siguiente lema muestra cuán acertada es esta definición.

Lema.

1) $.\langle u,v\rangle \in x \supset u \in \mathrm{Fld}(x) \wedge v \in \mathrm{Fld}(x)$;

2) $.\mathrm{Rel}(x) \wedge u \in \mathrm{Fld}(x) \supset \exists v(\langle u,v\rangle \in x \vee \langle v,u\rangle \in x)$.

► 1) Se cumple que $\{u,v\} \in \langle u,v\rangle \in x$, lo que significa que $\{u,v\} \in \cup x$. Luego, $u \in \{u,v\} \in \cup x$, de donde se deduce $u \in \cup\cup x$, es decir, $u \in \mathrm{Fld}(x)$. De la misma manera, $v \in \mathrm{Fld}(x)$.

2) Supongamos que $\mathrm{Rel}(x)$, $u \in \mathrm{Fld}(x)$. De esta manera, existe un v tal que $u \in v \in \cup x$. Por tanto, existe un z tal que $u \in v \in z \in x$. En virtud de $\mathrm{Rel}(x)$, existen v_1, v_2 tales que $z = \langle v_1, v_2\rangle$. En virtud de $v \in \langle v_1, v_2\rangle$, tenemos $v = \{v_1\}$ o $v = \{v_1, v_2\}$. Como resultado de que $u \in v$, necesariamente se cumple que $u = v_1$ o $u = v_2$. ◄

El *dominio de una relación* x es el conjunto de todos los elementos izquierdos de los pares de x:

$$\mathrm{dom}(x) \leftrightharpoons \{u \in \mathrm{Fld}(x) \mid \exists v(\langle u,v\rangle \in x)\}.$$

Ésta es una típica definición por comprehensión en ZF^+.

Señalemos que en virtud del lema, la restricción $u \in \mathrm{Fld}(x)$ en esta definición no es esencial:

$$.\exists\, v(\langle u, v\rangle \in x) \supset u \in \mathrm{Fld}(x).$$

En la matemática habitual se da una definición más sencilla:

$$\mathrm{dom}(x) = \{u \mid \exists\, v(\langle u, v\rangle \in x)\}.$$

Sin embargo, en el lenguaje que analizamos la última construcción es imposible, por lo que nos vemos en la necesidad de imponer una restricción, aunque la misma no es esencial.

Esta *restricción ficticia* en el axioma de comprehensión (particularidad de ZF^+) es el pago por la eliminación de las paradojas.

Propiedades fundamentales del dominio:

1) $.\langle u, v\rangle \in x \supset u \in \mathrm{dom}(x)$;
2) $.\mathrm{Rel}(x) \wedge u \in \mathrm{dom}(x) \supset \exists\, v(\langle u, v\rangle \in x)$.

► 2) Supongamos que $\mathrm{Rel}(x)$ y $u \in \mathrm{dom}(x)$. Entonces, según el axioma de comprehensión, obtenemos directamente $\exists\, v(\langle u, v\rangle \in x)$. ◄

$$.\mathrm{Rel}(x) \supset \mathrm{dom}(x) \subseteq \mathrm{Fld}(x).$$

El *rango* (*imagen*) de la relación x es el conjunto de todos los elementos derechos de los pares de x.

$$\mathrm{rng}(x) \leftrightharpoons \{v \in \mathrm{Fld}(x) \mid \exists\, u(\langle u, v\rangle \in x)\}.$$

1) $.\langle u, v\rangle \in x \supset v \in \mathrm{rng}(x)$;
2) $.\mathrm{Rel}(x) \wedge v \in \mathrm{rng}(x) \supset \exists\, u(\langle u, v\rangle \in x)$;
3) $.\mathrm{Rel}(x) \supset \mathrm{rng}(x) \cup \mathrm{dom}(x) = \mathrm{Fld}(x)$.

► Utilizar el lema para la demostración. ◄

1.3.3 El *producto cartesiano* de dos conjuntos x e y es una relación. Concretamente, éste es el conjunto de todos los pares $\langle u, v\rangle$ tales que $u \in x$, $v \in y$.

En el lenguaje M^+, el producto cartesiano podría ser definido de la siguiente manera:

$$x \times y \leftrightharpoons \{z \mid \exists uv(z = \langle u, v\rangle \wedge u \in x \wedge v \in y)\}.$$

En el lenguaje ZF^+, se necesita una condición (ficticia) restrictiva para poder definir el producto cartesiano por comprehensión. Es posible escribir

$$x \times y \leftrightharpoons \{z \in PP(x \cup y) \mid \exists uv(z = \langle u, v\rangle \wedge u \in x \wedge v \in y)\}.$$

En efecto, demostremos que de la condición escrita a la derecha de la barra vertical se deduce $z \in PP(x \cup y)$. Supongamos que para algunos u, v tenemos $z = \langle u, v\rangle$, $u \in x$, $v \in y$.

Entonces, $u \in x \cup y$ y $v \in x \cup y$. De aquí,

$$\{u\} \subseteq x \cup y, \quad \{v\} \subseteq x \cup y, \quad \{u, v\} \subseteq x \cup y.$$

Por tanto, obtenemos $\{u\} \in P(x \cup y)$, $\{u, v\} \in P(x \cup y)$. A su vez, de aquí resulta

$$\{\{u\}, \{u, v\}\} \subseteq P(x \cup y),$$

es decir, $\langle u, v\rangle \subseteq P(x \cup y)$ y, por tanto, $\langle u, v\rangle \in PP(x \cup y)$, es decir, $z \in PP(x \cup y)$.

Así pues, en el axioma de comprehensión la condición a la izquierda de la barra vertical se cumple si se cumple la condición a su derecha.

Proponemos demostrar a manera de ejercicio las propiedades fundamentales del producto cartesiano:

1) $.u \in x \wedge v \in y \supset \langle u, v\rangle \in x \times y$;

2) $.z \in x \times y \supset \exists\, uv(z = \langle u, v\rangle \wedge u \in x \wedge v \in y)$.

Diremos que una relación R está *definida en un conjunto* z si $R \subseteq z \times z$.

El siguiente lema indica cómo se determina el conjunto z.

Lema. $\mathrm{Rel}(R) \supset R \subseteq \mathrm{dom}(R) \times \mathrm{rng}(R)$.
De aquí, $R \subseteq z \times z$, *donde* $z = \mathrm{dom}(R) \cup \mathrm{rng}(R)$.

► Supongamos que $\mathrm{Rel}(R)$ e $y \in R$. Entonces, $y = \langle u, v\rangle$ y de las definiciones resulta $u \in \mathrm{dom}(R)$, $v \in \mathrm{rng}(R)$ y, en virtud de 1, resulta $y = \langle u, v\rangle \in \mathrm{dom}(R) \times \mathrm{rng}(R)$. ◄

1.3.4 Para toda relación R se puede definir la *relación inversa*, la cual está formada por los mismos pares, pero dispuestos en orden inverso. Esta relación se denota con R^{-1}, $\breve{R}$, o bien $\mathrm{Conv}(R)$. La definición exacta es la siguiente:

$$\mathrm{Conv}(R) \leftrightharpoons \{z \in \mathrm{rng}(R) \times \mathrm{dom}(R) \mid \exists\, uv(z = \langle u, v\rangle \wedge \langle v, u\rangle \in R)\}.$$

Señalemos que en este caso la restricción es ficticia.

1) $.\mathrm{Rel}(\mathrm{Conv}(R))$;

2) $.\langle u, v\rangle \in \mathrm{Conv}(R) \equiv \langle v, u\rangle \in R$.

1.3.5 Si están dadas dos relaciones, entonces puede ser definida su *composición*:

$$R \circ S \leftrightharpoons \{z \in \mathrm{dom}(S) \times \mathrm{rng}(R) \mid \exists\, uvw(z = \\ = \langle u, w\rangle \wedge \langle u, v\rangle \in S \wedge \langle v, w\rangle \in R)\}.$$

Propiedades fundamentales de la composición:

1) $.\mathrm{Rel}(R \circ S)$;

2) $.\langle u, v\rangle \in S \wedge \langle v, w\rangle \in R \supset \langle u, w\rangle \in R \circ S$;

3) $.\langle u, w\rangle \in R \circ S \supset \exists v(\langle u, v\rangle \in S \wedge \langle v, w\rangle \in R)$.

► Demostremos 3 (la demostración de las demás propiedades se propone al lector).

Si $\langle u, w\rangle \in R \circ S$, entonces, por definición,

$$\langle u, w\rangle \in \mathrm{dom}(S) \times \mathrm{rng}(R)$$

y, además, existen u', v', w', $\langle u, w\rangle = \langle u', w'\rangle$, $\langle u', v'\rangle \in S$, $\langle v', w'\rangle \in R$. En virtud de la subsección 1.3.1, $u = u'$, $w = w'$. Si definimos $v = v'$, entonces vemos que $\langle u, v\rangle \in S$, $\langle v, w\rangle \in R$. ◄

1.3.6 Introduzcamos los conceptos de *relación reflexiva, relación simétrica* y *relación transitiva.*

Recordemos que $xRy \leftrightharpoons \langle x, y\rangle \in R$.

$$\mathrm{Ref}(R) \leftrightharpoons (\forall x \in \mathrm{Fld}(R))(xRx);$$

$$\mathrm{Sym}(R) \leftrightharpoons \forall xy(xRy \supset yRx);$$

$$\mathrm{Trans}(R) \leftrightharpoons \forall xyz(xRy \wedge yRz \supset xRz).$$

Una relación se denomina *relación de equivalencia* si ella es al mismo tiempo reflexiva, simétrica y transitiva. La definición exacta es la siguiente:

$$\mathrm{Eq}(R) \leftrightharpoons \mathrm{Rel}(R) \wedge \mathrm{Ref}(R) \wedge \mathrm{Sym}(R) \wedge \mathrm{Trans}(R).$$

Ejercicio. Demostrar

$$.\mathrm{Rel}(R) \wedge \mathrm{Ref}(R) \supset \mathrm{Fld}(R) = \mathrm{dom}(R) = \mathrm{rng}(R).$$

1.3.7 Se denomina *restricción de una relación R a un conjunto x* al conjunto de los pares $\langle u, v\rangle$ de R tales que $u \in x$. La definición exacta es $R \restriction x \leftrightharpoons R \cap (x \times \mathrm{rng}(R))$.

$$.\langle u, v\rangle \in (R \restriction x) \equiv (\langle u, v\rangle \in R \wedge u \in x).$$

Se denomina *imagen de un conjunto x por una relación R* al conjunto de todos los v para los que existe un u perteneciente a x tal que $\langle u, v\rangle \in R$. La definición exacta es

$$R\text{“}x \leftrightharpoons R[x] \leftrightharpoons \{v \in \mathrm{rng}(R) \mid (\exists\, u \in x)(\langle u, v\rangle \in R)\}.$$

Ejercicio. Demostrar

$$.R\text{“}x = \mathrm{rng}(R \restriction x).$$

Se denomina *preimagen de un conjunto x por una relación R* (concepto simétrico al anterior) al conjunto de todos los u para los cuales existe un v perteneciente a x tal que $\langle u, v\rangle \in R$. La definición exacta es

$$R_{-1}x \leftrightharpoons \{u \in \mathrm{dom}(R) \mid (\exists\, v \in x)(\langle u, v\rangle \in R)\}.$$

Ejercicio. Demostrar

$$.\mathrm{Rel}(R) \supset R_{-1} = (R^{-1})\text{“}x.$$

De la misma manera se podría desarrollar la teoría de las relaciones n-arias. Por ejemplo, una relación ternaria es, por definición, un conjunto cuyos elementos son ternas ordenadas.

1.3.8 Se denomina *función* (de una variable) a toda relación que satisface la siguiente condición: si $\langle u, v_1\rangle \in R$ y $\langle u, v_2\rangle \in R$, entonces $v_1 = v_2$, es decir, para todo u del dominio de R existe

sólo un v que se encuentra con u en la relación R. La definición exacta es

$$\mathrm{Fnc}(R) \leftrightharpoons \mathrm{Rel}(R) \wedge \forall\, uv_1v_2(uRv_1 \wedge uRv_2 \supset v_1 = v_2).$$

El segundo término conjuntivo es conocido a veces como *condición de uniformidad* (respecto a la segunda coordenada). De esta manera, una función es una relación uniforme respecto a la segunda coordenada.

Diremos que una función f *aplica* el conjunto X en el conjunto Y, y escribiremos

$$f : X \to Y,$$

si el dominio de f es X, y el rango de f está incluido en Y:

$$f : X \to Y \leftrightharpoons \mathrm{Fnc}(f) \wedge \mathrm{dom}(f) = X \wedge \mathrm{rng}(f) \subseteq Y.$$

Diremos que una función f *transforma* x en y si $\langle x, y\rangle \in f$:

$$f : x \mapsto y \leftrightharpoons \mathrm{Fnc}(f) \wedge \langle x, y\rangle \in f.$$

Si $x \in \mathrm{dom}(f)$ y f es una función, entonces existe uno y sólo un y tal que $\langle x, y\rangle \in f$. Este y se denomina *valor de la función* f en x. Se puede dar la definición explícita del valor de una función en el lenguaje considerado:

$$f'x \leftrightharpoons f(x) \leftrightharpoons \cup\{y \in \mathrm{rng}(f) \mid \langle x, y\rangle \in f\}.$$

La propiedad fundamental de esta notación es

$$.\mathrm{Fnc}(f) \wedge x \in \mathrm{dom}(f) \supset ((z = f'x) \equiv (\langle x, z\rangle \in f)).$$

► Supongamos que $\mathrm{Fnc}(f)$ y $x \in \mathrm{dom}(f)$. Debido a que $x \in \mathrm{dom}(f)$, existe un u tal que $\langle x, u\rangle \in f$. Supongamos que $Q = \{y \in \mathrm{rng}(f) \mid \langle x, y\rangle \in f\}$. Por definición, $y \in Q \equiv \langle x, y\rangle \in f$. Pero según la condición de uniformidad, $\langle x, y\rangle \in f \wedge \langle x, y\rangle \in f \supset y = u$. Por tanto, $y \in Q \equiv (y = u)$. De aquí se deduce $Q = \{u\}$. Por tanto, $\cup Q = \cup\{u\} = u$. Pero $\cup Q$ es $f'x$, de modo que $f'x = u$. Si $z = f'x$, entonces $z = u$ y, por tanto, $\langle x, z\rangle \in f$. Y viceversa, si $\langle x, z\rangle \in f$, entonces, en virtud de $\langle x, u\rangle \in f$ y la condición de uniformidad, tenemos $z = u$, es decir, $z = f'x$. ◄

No se deben confundir las siguientes dos notaciones, cuyos sentidos son totalmente diferentes:

$f(x) \leftrightharpoons f'x$ — valor de la función f en x.

$f[\mathrm{x}] \leftrightharpoons f''x$ — imagen del conjunto x por la función f.

Análogamente, tienen sentidos diferentes las siguientes fórmulas:

$f : X \to Y$ — la función f aplica el conjunto X en el conjunto Y.

$f : x \mapsto y$ — la función f transforma x en y.

Nótese que toda función es también una relación, de modo que todas las definiciones concernientes a las relaciones pueden ser utilizadas para las funciones. Así pues, se definen el dominio de una función, el rango, la restricción de una función a un conjunto, la composición de funciones.

Lema. *La composición de dos funciones es una función:*

$$.\mathrm{Fnc}(f) \wedge \mathrm{Fnc}(g) \supset \mathrm{Fnc}(f \circ g).$$

► Supongamos que Fnc(f), Fnc(g). Comprobemos la condición de uniformidad para $f \circ g$. Supongamos que $\langle u, v_1\rangle \in f \circ g$, $\langle u, v_2\rangle \in f \circ g$, y demostremos que $v_1 = v_2$. Según la definición de composición, existen w_1 y w_2 tales que

$$\langle u, w_1\rangle \in g, \quad \langle w_1, v_1\rangle \in f$$

y

$$\langle u, w_2\rangle \in g, \quad \langle w_2, v_2\rangle \in f.$$

De la condición de uniformidad, para g tenemos $w_1 = w_2$. Pero entonces $v_1 = v_2$, de acuerdo con la condición de uniformidad para f. ◄

Lema. *El valor de la composición de funciones es igual al cálculo consecutivo de los valores de las funciones componentes:*

$$.\text{Fnc}(f) \wedge \text{Fnc}(g) \wedge x \in \text{dom}(g) \wedge (g'x) \in \text{dom}(f) \supset$$
$$\supset (f \circ g)'x = f'(g'x).$$

Préstese atención a que primeramente se calcula el valor de la función g (la de la derecha en la composición).

► Supongamos que $v = (f \circ g)'x$. Entonces $\langle x, v\rangle \in (f \circ g)$ y, por tanto, existe un w, $\langle x, w\rangle \in g$, $\langle w, v\rangle \in f$, de acuerdo con la definición de composición. Pero entonces $w = g'x$ y $v = f'w$, es decir, $v = f'(g'x)$. ◄

Para una función dada f, la relación inversa $f^{-1} = \text{Conv}(f)$ puede no ser una función. Una función f se denomina *función biunívoca* o *biyección* si la relación inversa es también una función:

$$(1-1)(f) \leftrightharpoons \text{Fnc}(f) \wedge \text{Fnc}(\text{Conv}(f)).$$

El conjunto de *todas las funciones* de un conjunto X en un conjunto Y se denota con $(X \to Y)$. De esta manera,

$$.f \in (X \to Y) \equiv f : X \to Y.$$

La definición por comprehensión es

$$(X \to Y) \leftrightharpoons \{f \in P(X \times Y) \mid f : X \to Y\}.$$

Ejercicio. Comprobar que la restricción $f \in P(X \times Y)$ es ficticia y se deduce de la condición $f : X \to Y$.

Es posible desarrollar de manera natural la teoría de funciones de varias variables. Por ejemplo, una función de dos variables es, por definición, una relación ternaria uniforme respecto a la última coordenada.

1.3.9 Sea $t(i)$ un término del lenguaje ZF^+ con variable destacada i. A veces escribiremos t_i en lugar de $t(i)$ para subrayar el papel particular de la variable i. Sea I un término arbitrario que no contiene apariciones libres de la variable i.

Se puede introducir la notación

$$\{t_i \mid i \in I\}$$

de modo que

$$.u \in \{t_i \mid i \in I\} \equiv (\exists\, i \in I)(u = t_i).$$

Esta notación se lee de la siguiente manera: «la familia de todos los t_i para $i \in I$».

Análogamente, para el término $t(i, j)$, con dos variables destacadas, se define la familia

$$\{t_{ij} \mid i \in I, j \in J\},$$

de modo que

$$.u \in \{t_{ij} \mid i \in I, j \in J\} \equiv (\exists\, i \in I)(\exists\, j \in J)(u = t_{ij}).$$

De manera similar se pueden definir familias de conjuntos respecto a términos con mayor número de variables destacadas.

▶ Estas notaciones se introducen con ayuda de la definición por reemplazo. Por ejemplo, sean $t(i, j)$ un término, i y j dos variables diferentes, e I y J dos términos cualesquiera que no contienen apariciones libres de las variables i y j. Definamos

$$\{t_{ij} \mid i \in I,\ j \in J\} \rightleftharpoons \{y \mid x \in I \times J,\ (x \mapsto y),\ \exists\, ij(x = \\ = \langle i, j\rangle \wedge y = t_{ij})\}.$$

Entonces (véase la subsección 1.1.12), $u \in \{t_{ij} \mid i \in I, j \in \in J\} \Leftrightarrow$ existe un $x \in I \times J$ tal que exactamente para un u se cumple

$$\exists\, ij(x = \langle i, j\rangle \wedge u = t_{ij}).$$

Pero para todo $x \in I \times J$ este u siempre existe y es único. En efecto, para $x \in I \times J$ se determinan unívocamente i y j, $x = \langle i, j\rangle$ y, por tanto, u se determina unívocamente a partir de la igualdad $u = t_{ij}$. De esta manera,

$$u \in \{t_{ij} \mid i \in I, j \in J\}$$

si y sólo si existen $i \in I$, $j \in J$, $u = t_{ij}$. ◀

Estas notaciones permiten de manera compacta y clara expresar en el lenguaje ZF^+ muchas construcciones frecuentemente utilizadas en la matemática habitual.

Por ejemplo,

$$U \times V = \{\langle u, v\rangle \mid u \in U, v \in V\},$$

aquí, u y v son las variables destacadas.

Nótese que las variables destacadas aparecen ligadas en esta notación.

Definamos la *unión de una familia de conjuntos*:

$$\bigcup_{i\in I} t_i \leftrightharpoons \bigcup\{t_i \mid i \in I\}.$$

La propiedad fundamental es

$$.z \in \bigcup_{i\in I} t_i \equiv (\exists\, i \in I)(z \in t_i).$$

▶ $z \in \bigcup_{i\in I} t_i \equiv z \in \bigcup\{t_i \mid i \in I\} \equiv (\exists\, u \in \{t_i \mid i \in I\})(z \in u) \equiv$

$\equiv \exists\, u(\exists\, i \in I)(u = t_i \wedge z = u) \equiv (\exists\, i \in I)(z \in t_i).$ ◀

Definamos la *intersección de una familia de conjuntos*:

$$\bigcap_{i\in I} t_i \leftrightharpoons \bigcap\{t_i \mid i \in I\}.$$

1) $I \neq \varnothing \supset .\, z \in \bigcap_{i\in I} t_i \equiv (\forall\, i \in I)(z \in t_i)$;

2) $\bigcap_{i\in\varnothing} t_i = \varnothing$.

▶ Véase la subsección 1.2.3. ◀

El *producto cartesiano de una familia de conjuntos* se define de la siguiente manera:

$$\prod_{i\in I} t_i \leftrightharpoons \{f \in (I \to \bigcup_{i\in I} t_i) \mid (\forall\, i \in I)((f'i) \in t_i)\}.$$

1.3.10 En la matemática habitual, a veces por función se entiende una expresión analítica dependiente de una variable. Por ejemplo, se habla de la «función» $x^2 + x + 1$. En un lenguaje exacto, a expresiones de este tipo **no les corresponden funciones, sino términos.** Un término no describe una función, sino sus valores.

Si deseamos formar una función con dominio z a partir del término $t(x)$, entonces esta función se definirá mediante otro término:

$$f = \{\langle x, t(x)\rangle \mid x \in z\}.$$

Para todo $x \in z$, tenemos

$$.f : x \mapsto t(x).$$

1.4 Los números naturales en la teoría de conjuntos. Escritura de las afirmaciones matemáticas en el lenguaje de la teoría de conjuntos

1.4.1 Consideremos la siguiente sucesión de conjuntos:

$$\varnothing, \quad \{\varnothing\}, \quad \{\varnothing, \{\varnothing\}\}, \quad \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \quad \ldots .$$

Esta sucesión se obtiene a partir del conjunto vacío aplicando sucesivamente la operación $Sx = x \cup \{x\}$:

$$\{\varnothing\} = S(\varnothing), \quad \{\varnothing, \{\varnothing\}\} = S(\{\varnothing\}), \text{ etcétera.}$$

El primer elemento de esta sucesión no contiene elementos; el segundo contiene un elemento; el tercero, dos; y así sucesivamente.

Préstese atención a una importante particularidad de esta sucesión: todo elemento es exactamente igual al conjunto

de todos los elementos anteriores de la sucesión. Por ejemplo, el elemento $\{\varnothing, \{\varnothing\}\}$ es antecedido por los elementos $\varnothing$ y $\{\varnothing\}$. Si ordenamos los elementos de esta sucesión considerando que $a < b \Leftrightarrow a$ precede a b en la sucesión, entonces para los elementos de esta sucesión se cumple

$$a < b \Leftrightarrow a \in b.$$

De esta manera, la relación de pertenencia define un *orden lineal* en esta sucesión.

Von Neumann propuso definir los *números naturales* en la teoría de conjuntos como elementos de la sucesión indicada anteriormente:

$$0 \leftrightharpoons \varnothing, \quad 1 \leftrightharpoons \{\varnothing\}, \quad 2 \leftrightharpoons \{\varnothing, \{\varnothing\}\}, \quad \ldots$$

y, en general, si se ha definido el número natural n, entonces el siguiente número es Sn.

Los *axiomas de infinitud* (véase la subsección 1.2.2) afirman precisamente que ω es el conjunto de los números naturales según Von Neumann. En efecto, las primeras dos afirmaciones,

$$\varnothing \in \omega, \quad (\forall x \in \omega)(Sx \in \omega),$$

declaran que ω contiene al menos todos los números naturales, mientras que la tercera afirmación,

$$\forall x(\mathrm{Prog}(x) \supset (\omega \subseteq x)),$$

asegura que ω es el «más pequeño» de los conjuntos que contienen todos los números naturales, es decir, hablando intuitivamente, sólo contiene números naturales.

Las tres afirmaciones siguientes expresan las propiedades fundamentales de los números naturales:

1) $.(\forall x \in \omega)(Sx \neq 0)$.
2) $.(\forall xy \in \omega)(Sx = Sy \equiv x = y)$.
3) Para toda fórmula $\varphi(x)$, se cumple la siguiente afirmación denominada *principio de inducción completa*:

$$.\varphi(0) \wedge (\forall x \in \omega)(\varphi(x) \supset \varphi(Sx)) \supset (\forall x \in \omega)\varphi(x).$$

► 1) Evidentemente, $x \in Sx = x \cup \{x\}$. Si se cumpliera $Sx = 0$, entonces $x \in \varnothing$, lo que es imposible.

3) Supongamos que $\varphi(0)$ y

$$(\forall x \in \omega)(\varphi(x) \supset \varphi(Sx))$$

y demostremos $(\forall x \in \omega)\varphi(x)$. Para esto, consideremos el conjunto $u = \{x \in \omega \mid \varphi(x)\}$. De las suposiciones hechas, se deduce que Prog(u). Por tanto, de acuerdo con los axiomas de infinitud tenemos $\omega \subseteq u$, lo que significa $(\forall x \in \omega)\varphi(x)$.

2) Para demostrar esto, necesitaremos demostrar dos afirmaciones auxiliares con ayuda del principio de inducción completa.

Primera afirmación:

$$(\forall x \in \omega)\, \forall yz(y \in z \wedge z \in x \supset y \in x).$$

Para $x = 0$, obtenemos la afirmación

$$\forall yz(y \in z \wedge z \in \varnothing \supset y \in \varnothing),$$

que es trivial, en virtud de la falsedad de la premisa $z \in \varnothing$. Consideremos ahora un número arbitrario $x \in \omega$; supongamos

$$\forall yz(y \in z \wedge z \in x \supset y \in x),$$

y demostremos

$$\forall yz(y \in z \wedge z \in Sx \supset y \in Sx).$$

Supongamos que $y \in z$, $z \in Sx$. De $z \in Sx$ se deduce $z \in x$ o $z = x$. En el primer caso, tenemos $y \in z$, $z \in x$ y, por tanto, $y \in x$ según la hipótesis de inducción. De aquí, resulta $y \in Sx$.

En el segundo caso, tenemos $y \in Sx$ en virtud de $z \in Sx$.

La primera afirmación queda demostrada.

Segunda afirmación:

$$\forall x(x \notin x).$$

Es evidente que $\varnothing \notin \varnothing$. Para $x \in \omega$, supongamos $x \notin x$, y demostremos $Sx \notin Sx$. Supongamos lo contrario, y $Sx \in Sx$. Entonces, $Sx \in x$ o $Sx = x$. En el primer caso, en virtud de $x \in Sx$ y de la primera afirmación, obtenemos $x \in x$, lo que contradice la hipótesis de inducción. En el segundo caso, en virtud de $x \in Sx$, concluimos inmediatamente que $x \in x$, lo que nuevamente contradice la hipótesis de inducción. La segunda afirmación ha sido demostrada.

Finalmente, demostremos 2. Supongamos que $Sx = Sy$, y demostremos que $x = y$ (la implicación inversa se deduce de las leyes generales de la igualdad). Puesto que $x \in Sx$, se cumple $x \in Sy$, es decir, $x \in y$ o $x = y$. En el segundo caso, la afirmación queda demostrada, de modo que es suficiente demostrar que el caso $x \in y$ es imposible. De $y \in Sy$ deducimos que $y \in Sx$, es decir, $y \in x$ o $y = x$. Pero si $x \in y$ e $y \in x$, entonces, según la primera afirmación auxiliar, tenemos $x \in x$, lo que contradice la segunda afirmación. ◄

Resulta que todo lo que se exige de los números naturales en la matemática, se puede deducir de las tres afirmaciones indicadas, denominadas *axiomas de Peano*. Los números naturales se pueden definir en la teoría de conjuntos de otra manera,

no necesariamente según Von Neumann, sólo es importante que se cumplan las afirmaciones 1–3.

Por ejemplo, de los axiomas de Peano con ayuda de los medios de ZF^+ se puede demostrar la existencia de las funciones de adición, multiplicación y elevación a una potencia para los números naturales, y deducir todas las propiedades habituales de estas funciones.

Más aún, los axiomas de Peano de hecho definen unívocamente el conjunto de los números naturales en ZF^+. Más exactamente, si existe un conjunto ω^*, un elemento $0^* \in \omega^*$ y una función S definida en ω^*, $S^* : \omega^* \to \omega^*$, y además, para 0^*, ω^* y S^*, se cumplen los axiomas de Peano, entonces existe un isomorfismo natural entre ω y ω^*, es decir, existe una función biunívoca $f : \omega \to \omega^*$ sobre todo el conjunto ω^* tal que $f'0 = 0^*$ y $f'(Sx) = S^*(f'x)$. Además, la función f es única. Como se dice, los axiomas de Peano *son categóricos en la teoría de conjuntos*, es decir, ellos definen unívocamente el conjunto de los números naturales si permitimos utilizar los medios de la teoría de conjuntos.

Las propiedades fundamentales de los números naturales y de los números reales se estudian en los libros de texto dedicados a los sistemas numéricos y al análisis matemático. Aquí no nos detendremos en esto, sólo analizaremos brevemente la definición del conjunto de todos los números reales, R, según el estilo de Dedekind.

Definamos primeramente el conjunto Rat_0, formado por las *notaciones canónicas para los números racionales*. A saber,

$$x \in \mathrm{Rat}_0 \equiv \exists\, uvw(x = \langle u, v, w\rangle \wedge (u = 0 \vee u = 1) \wedge v \in$$
$$\in \omega \wedge w \in \omega \wedge w \neq 0).$$

Si $x = \langle u, v, w\rangle$, entonces u se denomina *símbolo* de x; v, numerador de x; y w, denominador de x. Las ternas de la forma $\langle 0, v, w\rangle$ se denotan con v/w o $+v/w$, y las ternas de la forma $\langle 1, v, w\rangle$, con $-v/w$.

Definamos seguidamente la *relación natural de equivalencia* entre las notaciones canónicas de los números racionales:

$$\langle u, v, w\rangle =_r \langle u, v_1, w_1\rangle \leftrightharpoons v \cdot w_1 = v_1 \cdot w,$$

$$\langle 0, v, w\rangle =_r \langle 1, v_1, w_1\rangle \leftrightharpoons v = v_1 = 0.$$

Aquí, la multiplicación indicada a la derecha es la multiplicación habitual de números naturales.

El conjunto de todos los *números racionales*, Rat, se define como el conjunto Rat_0 de todas las clases de equivalencia respecto a esta relación de equivalencia. De una manera más formal,

$$\mathrm{Rat} \leftrightharpoons \{y \in P(\mathrm{Rat}_0) \mid (\exists\, z \in \mathrm{Rat}_0)\, \forall\, x(x \in y \equiv (x =_r z))\}.$$

Seguidamente, en el conjunto Rat se introducen de manera habitual todas las operaciones fundamentales con números racionales. Por ejemplo, la *multiplicación* de números racionales se describe de la siguiente manera (ésta es precisamente la regla de «multiplicación de fracciones», que estudiamos en la escuela):

$$x_1 \cdot_r x_2 \leftrightharpoons \{z \in \mathrm{Rat}_0 \mid \exists\, u u_1 v_1 w_1 u_2 v_2 w_2((\langle u_1, v_1, w_1\rangle \in x_1) \wedge$$

$$\wedge(\langle u_2, v_2, w_2\rangle \in x_2) \wedge (z =_r \langle u, v_1 \cdot v_2, w_1 \cdot w_2\rangle) \wedge$$

$$\wedge(u = 0 \vee u = 1) \wedge (u = 1 \equiv (u_1 \neq u_2)))\}.$$

Por supuesto, se debe comprobar que realmente esta operación, al ser aplicada a dos números racionales x_1 y x_2, nos da un número racional y, además, satisface las propiedades habituales de la multiplicación de números racionales. Si se desea,

se puede definir una constante, una función de dos argumentos, la *multiplicación de números racionales*:

$$\cdot_r \leftrightharpoons \{z \in \mathrm{Rat}^3 \mid (\exists\, x_1 x_2 x_3 \in \mathrm{Rat})(z = \langle x_1, x_2, x_3\rangle \wedge x_3 = x_1 \cdot_r x_2)\}.$$

En este caso tendremos

$$.(\forall\, x_1 x_2 \in \mathrm{Rat})(\,\cdot_r{}'\,\langle x_1, x_2\rangle = x_1 \cdot_r x_2).$$

De manera análoga se pueden definir las operaciones de adición $x +_r y$, sustracción $x -_r y$, el módulo $|x|_r$ de un número racional, así como la relación $x <_r y$, es decir, la desigualdad estricta de números racionales.

Como se sabe, se denomina *corte en la región de los números racionales* a toda partición del conjunto Rat en dos subconjuntos no vacíos X e Y tales que el conjunto X, junto con cada número contenido en él, también contiene todos los números menores que éste, mientras que el conjunto Y, junto con cada número contenido en él, también contiene todos los números mayores que éste. La definición de corte en este lenguaje es la siguiente:

$$\mathrm{Ct}(x) \leftrightharpoons (\exists\, X \subseteq \mathrm{Rat})(\exists\, Y \subseteq \mathrm{Rat})(x = \langle X, Y\rangle \wedge X \neq \varnothing \wedge$$
$$\wedge Y \neq \varnothing \wedge X \cup Y = \mathrm{Rat} \wedge X \cap Y = \varnothing \wedge$$
$$\wedge(\forall\, uv \in \mathrm{Rat})(u <_r v \supset (v \in X \supset u \in X) \wedge (u \in Y \supset v \in Y))).$$

Un corte $\langle X, Y\rangle$ se denomina *corte correcto* si en la clase inferior X de este corte no existe un número máximo. El concepto de corte correcto se puede describir mediante la siguiente fórmula:

$$\mathrm{CorCt}(x) \leftrightharpoons \mathrm{Ct}(x) \wedge \forall\, XY(x = \langle X, Y\rangle \supset$$
$$\supset (\forall\, u \in X)(\exists\, v \in X)(u <_r v)).$$

Ahora, según el esquema conocido, identificamos el conjunto R de todos los números reales con el conjunto de todos los cortes correctos:

$$\mathrm{R} \leftrightharpoons \{x \in P(\mathrm{Rat}) \times P(\mathrm{Rat}) \mid \mathrm{CorCt}(x)\}.$$

Ésta es una típica definición según el principio de comprehensión, donde a la izquierda de la barra vertical se tiene una restricción ficticia.

Seguidamente, en el conjunto R se deben definir todas las operaciones habituales con números reales. Por ejemplo, la relación de desigualdad estricta se puede introducir de la siguiente manera:

$$\langle X_1, Y_1\rangle < \langle X_2, Y_2\rangle \leftrightharpoons Y_1 \cap X_2 \neq \varnothing.$$

1.4.2 Aquí no nos dedicaremos al desarrollo de la teoría de los números reales y admitiremos que en ZF^+ pueden ser definidos el conjunto R de todos los números reales y todas las operaciones habituales con números reales, a saber, la adición, la multiplicación, el módulo de los números reales, etcétera.

Recordemos la definición de los cuantificadores limitados (véase la subsección 1.1.8):

$$(\forall\, x \in y)\varphi(x) \leftrightharpoons \forall\, x(x \in y \supset \varphi(x));$$

$$(\exists\, x \in y)\varphi(x) \leftrightharpoons \exists\, x(x \in y \wedge \varphi(x)).$$

Aparte de ser compacta, la importancia de esta definición radica en que los cuantificadores limitados se comportan en muchos aspectos de manera similar a los cuantificadores habituales, sobre todo si $y \neq \varnothing$. Por ejemplo, para los cuantificadores limitados tiene lugar una ley análoga a las leyes de De Morgan.

Además,

$$.y \neq \varnothing \supset ((\forall\, x \in y)\varphi(x) \supset (\exists\, x \in y)\varphi(x)).$$

Introduzcamos algunas abreviaciones más. Fijemos cierto conjunto u, $u \neq \varnothing$. En el lenguaje ZF^+, este conjunto puede ser representado, por ejemplo, mediante un término cerrado. Tomemos ahora un conjunto F de variables $a, b, c, \ldots$; supongamos que ellas *recorren los elementos del conjunto* u. De una manera más formal, esto significa lo siguiente:

1) en cada demostración, al considerar un elemento a representado mediante una variable del conjunto F, supondremos automáticamente que es válido $.a \in u$;
2) en toda fórmula, los cuantificadores

$$\forall\, a\varphi(a), \quad \exists\, a\varphi(a)$$

se deben interpretar como limitados:

$$(\forall\, a \in u)\varphi(a), \quad (\exists\, a \in u)\varphi(a);$$

3) los términos de la forma $\{a \mid \varphi(a)\}$ se deben interpretar como $\{a \in u \mid \varphi(a)\}$.

Resumiendo, omitimos en todas partes la restricción $\in u$ si se trata de variables del conjunto F. Por supuesto, si es necesario, esta restricción debe ser restablecida. Si la variable se toma del conjunto F, esto se considera indicación de que se debe agregar la restricción.

Este método de uso de las variables se denomina *introducción de variables subordinadas* .Diremos que las variables de la lista F *están sometidas a la condición* $\in u$.

Por ejemplo, convenimos en utilizar las letras $m, n, k, \ldots$, posiblemente con índices, para denotar los *números naturales*, es decir, las variables del conjunto $m, n, k, \ldots$ se someten a la condición $\in \omega$.

Utilizando estas notaciones, el principio de inducción completa se escribe de la siguiente manera:

$$\varphi(0) \wedge \forall m(\varphi(m) \supset \varphi(Sm)) \supset \forall m\varphi(m).$$

En una forma más detallada, tenemos

$$\varphi(0) \wedge (\forall m \in \omega)(\varphi(m) \supset \varphi(Sm)) \supset (\forall m \in \omega)\varphi(m).$$

Ejercicio. Analizar las siguientes definiciones:

1) a es una sucesión de números reales:

$$(a : \omega \to R).$$

2) b es una subsucesión de la sucesión a:

$$(a : \omega \to R) \wedge (b : \omega \to R) \wedge$$
$$\wedge(\exists f \in (\omega \to \omega)) \forall m((f'm < f'Sm) \wedge (b'm = a'(f'm))).$$

En lo sucesivo utilizaremos las letras $\alpha, \beta, \gamma, \delta, \varepsilon, \ldots$ (posiblemente, con índices) para denotar los números reales, es decir, someteremos las variables de este conjunto a la condición $\in R$.

Definición de intervalo $[\alpha, \beta]$ de números reales:

$$[\alpha, \beta] \rightleftharpoons \{\gamma \mid \alpha \leqslant \gamma \wedge \gamma \leqslant \beta\}.$$

Definición de función f continua en un punto α del intervalo $[0, 1]$:

$$(f : [0,1] \to R) \wedge \alpha \in [0,1] \wedge (\forall \varepsilon > 0)(\exists \delta > 0)$$
$$(\forall \beta \in [0,1])(|\alpha - \beta| < \delta \supset |f'\alpha - f'\beta| < \varepsilon).$$

Definición de función f continua en todo punto del intervalo $[0,1]$:

$$(f : [0,1] \to R) \wedge (\forall \varepsilon > 0)(\forall \alpha \in [0,1])(\exists \delta > 0)$$
$$(\forall \beta \in [0,1])(|\alpha - \beta| < \delta \supset |f'\alpha - f'\beta| < \varepsilon).$$

Definición de función f uniformemente continua en el intervalo $[0,1]$:

$$(f : [0,1] \to R) \wedge (\forall \varepsilon > 0)(\exists \delta > 0)(\forall \alpha \in [0,1])$$
$$(\forall \beta \in [0,1])(|\alpha - \beta| < \delta \supset |f'\alpha - f'\beta| < \varepsilon).$$

Nótese que el orden de los cuantificadores que se refieren a δ y a α es diferente en las definiciones de continuidad y continuidad uniforme. En esta permutación de cuantificadores radica la diferencia esencial entre la continuidad y la continuidad uniforme.

El conocimiento de las leyes lógicas nos permite ahora transformar rápidamente las fórmulas a la forma necesaria. Por ejemplo, formulemos la afirmación «la función f no es uniformemente continua en el intervalo $[0,1]$» de manera que la negación no figure en la afirmación. Para esto, en la definición de *continuidad uniforme* se debe colocar la negación delante del segundo término de la conjunción, a continuación aplicar las leyes de DeMorgan, la negación de la implicación y finalmente introducir la negación. Como resultado obtenemos:

$$(f : [0,1] \to R) \wedge (\exists \varepsilon > 0)(\forall \delta > 0)(\exists \alpha \in [0,1])$$
$$(\exists \beta \in [0,1])(|\alpha - \beta| < \delta \wedge |f'\alpha - f'\beta| \geqslant \varepsilon).$$

1.4.3 Todo esto hace que surja la idea correcta de que casi toda afirmación matemática puede ser escrita como una fórmula de ZF^+, y que el nombre de todo objeto matemático puede ser escrito en forma de un término de este lenguaje.

Veamos un ejemplo más. Como se sabe, se denomina *espacio topológico* a todo conjunto no vacío X en el que está definida una familia S de subconjuntos, denominados *conjuntos abiertos*, y además

1) $\varnothing$ y X son conjuntos abiertos;
2) la intersección de cualesquiera dos conjuntos abiertos también es un conjunto abierto;
3) la unión de una familia de conjuntos abiertos es un conjunto abierto.

En el lenguaje considerado, «ser un espacio topológico» se puede escribir mediante la siguiente fórmula:

$$\mathrm{Top}(x) \leftrightharpoons \exists X\, S(x = \langle X, S\rangle \wedge X \neq \varnothing \wedge S \subseteq P(X) \wedge \varnothing \in S \wedge$$
$$\wedge X \in S \wedge (\forall yz \in S)(y \cap z \in S) \wedge (\forall u \subseteq S)(\cup u \in S)).$$

1.4.4 Como hemos señalado, el lenguaje ZF^+ no es un lenguaje de primer orden debido a la estructura especial de sus términos. Consideremos el *lenguaje de primer orden* ZF. Este lenguaje contiene un tipo de variables para los conjuntos $(x, y, z, \ldots)$ y un predicado atómico único, $\in$. El lenguaje ZF no contiene constantes ni símbolos de función.

El lenguaje ZF es parte del lenguaje ZF^+. No obstante, como veremos, toda fórmula de ZF^+ es equivalente a cierta fórmula de ZF. En este sentido, los términos no son elementos necesarios

del lenguaje de la teoría de conjuntos y han sido introducidos por nosotros sólo para hacer más cómoda la notación de las afirmaciones matemáticas. En la lógica matemática, precisamente el lenguaje ZF es el que más a menudo se utiliza. A saber, para toda fórmula φ del lenguaje ZF^+ se define una fórmula φ^0 del lenguaje ZF con los mismos parámetros y tal que $\varphi \equiv \varphi^0$. En lo que respecta a los términos del lenguaje ZF^+, para toda fórmula de ZF^+ de la forma $y = t$, donde t es un término e y es una variable que no aparece libre en t, se define la fórmula $(y = t)^*$ de ZF de manera que

$$.(y = t) \equiv (y = t)^*.$$

Las fórmulas φ^0 y $(y = t)^*$ se definen por inducción simultánea de acuerdo con la definición de fórmulas y términos de la subsección 1.2.1:

1) $(y = x)^* \leftrightharpoons (y = x)$;

2) $(t \in r)^0 \leftrightharpoons \exists\, y_1 y_2((y_1 = t^* \wedge (y_2 = r)^* \wedge (y_1 \in y_2))$;

3) $(\varphi \wedge \psi)^0 \leftrightharpoons \varphi^0 \wedge \psi^0$;
$(\varphi \vee \psi)^0 \leftrightharpoons \varphi^0 \vee \psi^0$;
$(\varphi \supset \psi)^0 \leftrightharpoons \varphi^0 \supset \psi^0$;
$(\neg\varphi)^0 \leftrightharpoons \neg\varphi^0$;

4) $(\forall\, x\varphi)^0 \leftrightharpoons \forall\, x\varphi^0$;
$(\exists\, x\varphi)^0 \leftrightharpoons \exists\, x\varphi^0$;

5) $(y = \varnothing)^* \leftrightharpoons \forall\, x(x \notin y)$;
$\mathrm{Prog}^0(x) \leftrightharpoons \exists\, u(\forall\, v(v \notin u) \wedge u \in x) \wedge$
$\wedge(\forall\, u \in x)(\exists\, v \in x) \forall\, z(z \in v \equiv (z \in u \vee z = u))$;
$(y = \omega)^* \leftrightharpoons \mathrm{Prog}^0(y) \wedge \forall\, x(\mathrm{Prog}^0(x) \supset y \subseteq x)$;

6) $(y = \{t, r\})^* \leftrightharpoons \exists\, y_1 y_2((y_1 = t)^* \wedge (y_2 = r)^* \wedge \forall\, z(z \in y \equiv$
$\equiv (z = y_1 \vee z = y_2)))$;

7) $(y = Pt)^* \leftrightharpoons \exists\, y_1((y_1 = t)^* \wedge \forall\, z(z \in y \equiv z \subseteq y_1))$;
$(y = \cup t)^* \leftrightharpoons \exists\, y_1((y_1 = t)^* \wedge \forall\, z(z \in y \equiv (\exists\, v \in y_1)(z \in v)))$;

8) $(y = \{x \in t \mid \varphi(x)\})^* \leftrightharpoons \exists\, y_1((y_1 = t)^* \wedge\ \forall\, z(z \in y \equiv (z \in$
$\in y_1 \wedge \varphi^0(z))))$;

9) $(y = \{v \mid u \in t,\ (u \mapsto v),\ \varphi(u, v)\})^* \leftrightharpoons \exists\, y_1((y_1 = t)^* \wedge$
$\forall\, v(v \in y \equiv (\exists\, u \in y_1)(\varphi^0(u, v) \wedge \forall\, w(\varphi^0(u, w) \supset u = w))))$.

Utilizando este extenso procedimiento inductivo, para cada fórmula φ de ZF^+ se puede obtener la fórmula equivalente φ^0 de ZF. La demostración de la equivalencia se efectúa directamente por inducción y no nos detendremos en ella.

1.5 Sobre la hipótesis del continuo y el axioma de elección

1.5.1 Dos conjuntos se denominan *equipotentes* si existe una biyección que aplica un conjunto sobre el otro:

$$x \simeq y \leftrightharpoons \exists f((1-1)(f) \wedge \mathrm{dom}(f) = x \wedge \mathrm{rng}(f) = y).$$

Un conjunto se denomina *finito* si es equipotente a cierto número natural (recordemos que en la teoría de conjuntos cada número natural se identifica con el conjunto de todos los números que le preceden):

$$\mathrm{Fin}(x) \leftrightharpoons (\exists n \in \omega)(x \simeq n).$$

Un conjunto se llama *numerable* si es equipotente al conjunto de todos los números naturales:

$$\mathrm{Count}(x) \leftrightharpoons x \simeq \omega.$$

1.5.2 **Teorema** (Cantor).

$$.\neg(x \simeq Px).$$

► Supongamos lo contrario, $x \simeq Px$. Entonces existe una biyección f, $\operatorname{dom} f = x$, $\operatorname{rng} f = Px$. Consideremos el conjunto v,

$$v = \{z \in x \mid z \notin f'z\}.$$

Es evidente que $v \subseteq x$, es decir, $v \in Px$. Además, por definición,

$$(\forall z \in x)(z \in v \equiv z \notin (f'z)).$$

Puesto que f es una biyección, existe un $z_0 \in x$ tal que $f'z_0 = v$.

Sustituyamos en la equivalencia anterior z por z_0 y, puesto que $f'z_0 \notin v$, obtenemos

$$z_0 \in v \equiv z_0 \notin v,$$

lo que es imposible de acuerdo con las leyes de la lógica.

Préstese atención a la analogía entre este razonamiento y el razonamiento en la paradoja de Russell. ◄

Corolario. *El conjunto de todos los subconjuntos de números naturales no es numerable:*

$$.\neg\mathrm{Count}(P\omega).$$

1.5.3 La célebre *hipótesis del continuo* de Cantor se puede formular de la siguiente manera: toda familia de subconjuntos del conjunto de los números naturales es, o bien finita, o bien numerable, o bien equipotente al conjunto de todos los subconjuntos del conjunto de los números naturales. La formulación exacta es

$$(\forall y \subseteq P\omega)(\mathrm{Fin}(y) \vee \mathrm{Count}(y) \vee y \simeq P\omega).$$

La idea de esta afirmación radica en que no existen conjuntos infinitos de potencia estrictamente intermedia entre las potencias de los conjuntos ω y $P\omega$.

Como demostraron Gödel y Cohen, la hipótesis del continuo no depende de los demás axiomas de ZF, es decir, utilizando los medios de la lógica ella no puede ser demostrada ni refutada con ayuda de los demás axiomas, incluso si se incluye el axioma de elección.

1.5.4 El *axioma de elección* afirma que para toda familia x de conjuntos existe una función f tal que si $z \in x$ y $z \notin \varnothing$, entonces el valor de f para z es un elemento de z. La función f puede ser llamada *función de elección*, ella «elige» un elemento $(f'z) \in z$ de cada conjunto z, $z \in x$, $z \notin \varnothing$.

La formulación exacta del axioma de elección es la siguiente:

$$\forall x \exists f(\mathrm{Fnc}(f) \wedge \mathrm{dom}(f) = x \wedge (\forall z \in x)(z \notin \varnothing \supset (f'z) \in z)).$$

¿Es verdadera o no esta afirmación?

La particularidad de esta afirmación es que la función f no está definida por el conjunto x: sólo se afirma su existencia. Los teoremas obtenidos utilizando el axioma de elección tienen a menudo esta misma particularidad: se demuestra la existencia de un conjunto que posee cierta propiedad, pero no se indica ningún ejemplo concreto, ni se da ningún método para hallarlo. Un ejemplo típico es la demostración de la existencia de conjuntos no medibles. Como consecuencia, muchos matemáticos sometieron a crítica el uso ilimitado del axioma de elección.

Sin embargo, en los razonamientos matemáticos prácticos, el axioma de elección se utiliza ampliamente. Como demostraron

Gödel y Cohen, el axioma de elección también es independiente de los axiomas de ZF.

En la siguiente sección le daremos un carácter más específico al planteamiento general del problema sobre la independencia de las afirmaciones respecto a la teoría.

1.5.5 Diremos que la potencia de un conjunto x es menor o igual que la potencia de un conjunto y si x puede ser aplicado biunívocamente sobre el subconjunto y. Más exactamente,

$$x \widetilde{\subset} y \leftrightharpoons \exists f((1-1)(f) \wedge \mathrm{dom}(f) = x \wedge \mathrm{rng}(f) \subseteq y).$$

Teorema (Cantor—Schröder—Bernstein). *Si* $x \widetilde{\subset} y$ *e* $y \widetilde{\subset} x$, *entonces* $x \simeq y$.

► Es suficiente demostrar que si $a_1 \subseteq b \subseteq a$ y $a_1 \simeq a$, entonces $b \simeq a$. Supongamos que $(1-1)(f)$, $\mathrm{dom}(f) = a$ y $\mathrm{rng}(f) = a_1$. Tomemos

$$a_0 = a, \quad a_1 = f''a_0, \quad a_2 = f''a_1, \quad \ldots,$$
$$b_0 = b, \quad b_1 = f''b_0, \quad b_2 = f''b_1, \quad \ldots.$$

Definamos $g(x) = f(x)$ si $x \in a_n \setminus b_n$ para algún n; en caso contrario, $g(x) = x$. Entonces, $(1-1)(g)$, $\mathrm{dom}(g) = a$, $\mathrm{rng}(g) = b$. ◄

Ejercicio. Demostrar

$$.x \widetilde{\subset} y \wedge y \widetilde{\subset} z \supset x \widetilde{\subset} z.$$

1.5.6 **Nota.** Aparte de los conjuntos, en la matemática práctica a veces se utilizan las *clases*.

Consideremos una fórmula arbitraria $\varphi(x)$ del lenguaje ZF^+ en la que se ha elegido la variable x. Por conveniencia, consideremos

La idea de esta afirmación radica en que no existen conjuntos infinitos de potencia estrictamente intermedia entre las potencias de los conjuntos ω y $P\omega$.

Como demostraron Gödel y Cohen, la hipótesis del continuo no depende de los demás axiomas de ZF, es decir, utilizando los medios de la lógica ella no puede ser demostrada ni refutada con ayuda de los demás axiomas, incluso si se incluye el axioma de elección.

1.5.4 El *axioma de elección* afirma que para toda familia x de conjuntos existe una función f tal que si $z \in x$ y $z \notin \varnothing$, entonces el valor de f para z es un elemento de z. La función f puede ser llamada *función de elección*, ella «elige» un elemento $(f'z) \in z$ de cada conjunto z, $z \in x$, $z \notin \varnothing$.

La formulación exacta del axioma de elección es la siguiente:

$$\forall x \exists f(\mathrm{Fnc}(f) \wedge \mathrm{dom}(f) = x \wedge (\forall z \in x)(z \notin \varnothing \supset (f'z) \in z)).$$

¿Es verdadera o no esta afirmación?

La particularidad de esta afirmación es que la función f no está definida por el conjunto x: sólo se afirma su existencia. Los teoremas obtenidos utilizando el axioma de elección tienen a menudo esta misma particularidad: se demuestra la existencia de un conjunto que posee cierta propiedad, pero no se indica ningún ejemplo concreto, ni se da ningún método para hallarlo. Un ejemplo típico es la demostración de la existencia de conjuntos no medibles. Como consecuencia, muchos matemáticos sometieron a crítica el uso ilimitado del axioma de elección.

Sin embargo, en los razonamientos matemáticos prácticos, el axioma de elección se utiliza ampliamente. Como demostraron

Gödel y Cohen, el axioma de elección también es independiente de los axiomas de ZF.

En la siguiente sección le daremos un carácter más específico al planteamiento general del problema sobre la independencia de las afirmaciones respecto a la teoría.

1.5.5 Diremos que la potencia de un conjunto x es menor o igual que la potencia de un conjunto y si x puede ser aplicado biunívocamente sobre el subconjunto y. Más exactamente,

$$x \widetilde{\subset} y \leftrightharpoons \exists f((1-1)(f) \wedge \operatorname{dom}(f) = x \wedge \operatorname{rng}(f) \subseteq y).$$

Teorema (Cantor—Schröder—Bernstein). *Si* $x \widetilde{\subset} y$ *e* $y \widetilde{\subset} x$, *entonces* $x \simeq y$.

► Es suficiente demostrar que si $a_1 \subseteq b \subseteq a$ y $a_1 \simeq a$, entonces $b \simeq a$. Supongamos que $(1-1)(f)$, $\operatorname{dom}(f) = a$ y $\operatorname{rng}(f) = a_1$. Tomemos

$$a_0 = a, \quad a_1 = f''a_0, \quad a_2 = f''a_1, \quad \ldots,$$
$$b_0 = b, \quad b_1 = f''b_0, \quad b_2 = f''b_1, \quad \ldots.$$

Definamos $g(x) = f(x)$ si $x \in a_n \setminus b_n$ para algún n; en caso contrario, $g(x) = x$. Entonces, $(1-1)(g)$, $\operatorname{dom}(g) = a$, $\operatorname{rng}(g) = b$. ◄

Ejercicio. Demostrar

$$.x \widetilde{\subset} y \wedge y \widetilde{\subset} z \supset x \widetilde{\subset} z.$$

1.5.6 **Nota.** Aparte de los conjuntos, en la matemática práctica a veces se utilizan las *clases*.

Consideremos una fórmula arbitraria $\varphi(x)$ del lenguaje ZF^+ en la que se ha elegido la variable x. Por conveniencia, consideremos

que esta fórmula siembre define el objeto de investigación $\{x \mid \varphi(x)\}$. Este objeto se denomina *clase* de todos los conjuntos x que satisfacen la condición $\varphi(x)$.

Para algunas fórmulas $\varphi(x)$ de tipo especial, la clase $\{x \mid \varphi(x)\}$ es un conjunto; en el caso general, el concepto de clase es más amplio que el concepto de conjunto. Por ejemplo, $\{x \mid x \notin x\}$ es una clase que no es un conjunto, es decir, una *clase propia*. Hablando intuitivamente, las clases propias son agrupaciones «enormes» de potencia indefinida. Los elementos de una clase siempre son conjuntos (y no clases propias). Por analogía con los conjuntos, en las clases también se pueden definir algunas operaciones de la teoría de conjuntos. Por ejemplo, si tenemos las clases

$$X = \{x \mid \varphi(x)\}, \quad Y = \{y \mid \psi(y)\},$$

entonces se puede definir la clase

$$X \cup Y = \{x \mid \varphi(x) \vee \psi(x)\}.$$

Se puede formar la clase V de todos los conjuntos, que es una clase propia (no es un conjunto), el *universo* de la teoría de conjuntos.

La familia de los conjuntos forma una estructura tan potente que en la matemática práctica no hay necesidad real de utilizar las clases propias. Por lo general, se puede evitar mencionar directamente las clases si se consideran en su lugar las condiciones que las definen. No obstante, también se investigan lenguajes y teorías que contienen clases, como es el caso de la conocida teoría de Gödel—Bernays—Von Neumann, por ejemplo.

1.6 Teoría axiomática de conjuntos de Zermelo—Fraenkel

1.6.1. En la sección 1.1 se introdujo el lenguaje lógico-matemático de la teoría ingenua de conjuntos y comenzamos a desarrollar sistemáticamente la teoría de conjuntos en forma de una serie de afirmaciones de este lenguaje. Las demostraciones de las afirmaciones eran informales, «ingenuas». Nosotros partíamos de la idea de cierta estructura $\mathcal{U}$ cuyos objetos se denominan *conjuntos*. En esta estructura se cumplen leyes simples y naturales relacionadas con los conjuntos. Las afirmaciones eran demostradas (digámoslo así) mediante el estudio directo de esta estructura imaginaria, más exactamente, de las condiciones-axiomas impuestas a ella. Este enfoque es absolutamente natural para un matemático no especializado en lógica matemática.

Sin embargo, un análisis más cuidadoso demostró que los axiomas propuestos conllevaban a contradicciones y paradojas. Se tuvo que reconocer que, por lo visto, no existen estructuras que satisfacen las leyes propuestas por la teoría ingenua de conjuntos. Como salida de esta situación se consideró una estructura

más restringida $\mathcal{M}_0$, que satisface condiciones más estrictas y mucho menos naturales, expresadas en un lenguaje más complejo, ZF^+. Las demostraciones de las afirmaciones, no obstante, continuaban siendo ingenuas, como antes.

Surgen algunas preguntas. ¿Será «legal» considerar la estructura $\mathcal{M}_0$? ¿No nos llevarán nuevamente nuestros razonamientos a paradojas? ¿No se tendrá que reconocer que la estructura tampoco existe? Y acaso si es «legal» considerar la estructura $\mathcal{M}_0$, ¿será válido en $\mathcal{M}_0$ el axioma de elección, por ejemplo? En la matemática teórico-conjuntista moderna se ha acumulado una gran cantidad de problemas que obstinadamente no se someten a solución con ayuda de medios teórico-conjuntistas habituales, es decir, ellos no pueden ser demostrados ni refutados. ¿Sucede esto debido únicamente a la dificultad del problema y a la insuficiencia de los esfuerzos dedicados a su resolución, o es que el problema considerado no se puede ni demostrar ni refutar?

La solución de este tipo de problemas tropieza con la dificultad del estudio de la *semántica* de las teorías analizadas, es decir, la dificultad del estudio del método de comprensión de las fórmulas de la teoría. La semántica de las teorías matemáticas de alto contenido, como el análisis matemático, la teoría de conjuntos y otras, es por necesidad insuficientemente clara, tiene un carácter parcialmente filosófico en ocasiones. En lugar de describir un modelo concreto de la teoría, en estos casos nos vemos en la necesidad de limitarnos a la formulación de los *axiomas* (*convenios semánticos*) que deben ser satisfechos por esta teoría. Para el estudio de las teorías matemáticas de contenido abundante y semántica compleja, se puede aplicar exitosamente el *método de formalización de Hilbert*. Este método consiste en

que sobre la base de los convenios semánticos de una teoría informal $\mathscr{T}$ se construye una teoría axiomática formal T. En este caso, se trata de que los axiomas y las reglas de inferencia de T concuerden con las exigencias semánticas de $\mathscr{T}$. Entonces, las fórmulas deducibles según las reglas formales de la teoría T serán verdaderas informalmente desde el punto de vista de la teoría $\mathscr{T}$ y, de esta manera, reflejan al menos un fragmento de la teoría informal $\mathscr{T}$. Sería conveniente que, por supuesto, este fragmento fuera suficientemente extenso y abarcara todos los aspectos que nos interesan en la teoría $\mathscr{T}$. Más adelante, la teoría formal T puede ser sometida a una investigación matemática exacta y, de esta manera, se hace posible hacer conclusiones acerca de la semántica de la teoría informal inicial.

Una circunstancia muy importante es que para comprender la relación de argumentación formal $T \vdash A$ *no hay necesidad* de estudiar profundamente la semántica de la teoría $\mathscr{T}$ (que posiblemente es demasiado compleja): para demostrar $T \vdash A$ es suficiente construir un árbol de deducción, es decir, describir un objeto sintáctico simple formado por filas de símbolos dispuestos según reglas estrictamente definidas. La relación $T \vdash A$ se puede describir, por lo general, en una teoría suficientemente simple, por ejemplo, en la *aritmética formal* Ar, esto es, la teoría de los números naturales.

La formalización de las teorías permite darles un carácter más específico a los problemas semánticos dándoles la forma de afirmaciones sintácticas sobre las teorías formales.

Una teoría T en el lenguaje Ω se denomina *consistente* si no existe una sentencia (es decir, una fórmula del lenguaje Ω sin parámetros) tal que $T \vdash A$ y $T \vdash \neg A$.

Ejercicio. Demostrar que una teoría T es consistente si y sólo si existe una fórmula del lenguaje Ω que no es deducible en T.

Una teoría T se denomina *completa* si para toda sentencia A del lenguaje Ω tenemos, o bien $T \vdash A$, o bien $T \vdash \neg A$.

Diremos que una sentencia A es *compatible con la teoría* T si de la consistencia de la teoría T se deduce la consistencia de la teoría $T + A$, que se obtiene si se añade a la teoría T la fórmula A como axioma no lógico.

Ejercicio. Demostrar que A es compatible con T si y sólo si de la consistencia de la teoría T se deduce que es no válido $T \vdash \neg A$.

Una sentencia se denomina *independiente de la teoría* T si las sentencias A y $\neg A$ son compatibles con T.

Ejercicio. Demostrar que una sentencia A es independiente de la teoría T si y sólo si de la consistencia de la teoría T se deduce que en T no son deducibles ni la sentencia A ni la sentencia $\neg A$.

1.6.2 Formulemos ahora la teoría axiomática formal de Zermelo—Fraenkel. Ésta es una teoría en el lenguaje de primer orden ZF, es decir, en un lenguaje sin términos complejos. Denotemos esta teoría axiomática con ZF.

Describamos los axiomas no lógicos de ZF. Ellos se formulan paralelamente a los convenios semánticos expresados en la subsección 1.2.2. Si más adelante, en la formulación del axioma, figuran parámetros, entonces, como siempre, se debe considerar que el axioma es la clausura de una fórmula con cuantificadores universales referidos a todos los parámetros. Un axioma no lógico de una teoría es siempre una sentencia, una fórmula cerrada de esta teoría.

1) Axioma de extensionalidad:

$$x = y \wedge x \in z \supset y \in z.$$

2) Axioma del conjunto vacío:

$$\exists u \forall z(z \notin u).$$

3) Axioma del par no ordenado:

$$\exists u \forall z(z \in u \equiv (z = x \vee z = y)).$$

4) Axioma de la suma (unión):

$$\exists u \forall z(z \in u \equiv (\exists v \in x)(z \in v)).$$

5) Axioma del conjunto potencia:

$$\exists u \forall z(z \in u \equiv (z \subseteq x)).$$

6) Axioma de infinitud:

$$\exists u(\forall z(\forall x(x \notin z) \supset z \in u) \wedge (\forall z \in u) \\ (\forall v(\forall x(x \in v \equiv (x \in z \vee x = z)) \supset v \in u))).$$

7) Axioma de comprehensión:

$$\exists u \forall z(z \in u \equiv (z \in x \wedge \varphi(z))),$$

donde $\varphi(z)$ es una fórmula arbitraria del lenguaje ZF que no contiene apariciones libres de la variable u.

8) Axioma de reemplazo:

$$\exists u \forall z(z \in u \equiv (\exists x \in v)(\varphi(x, z) \wedge \forall w(\varphi(x, w) \supset z = w))),$$

donde $\varphi(x, z)$ es una fórmula que no contiene apariciones libres de las variables u y v.

9) Axioma de regularidad (o axioma de fundación):

$$\exists\, z(z \in x) \supset (\exists\, z \in x)\neg\exists\, u(u \in z \wedge u \in x).$$

Ésta es la formulación de la teoría ZF.

Los axiomas 2–8 expresan la existencia de los conjuntos que se representan directamente mediante términos del lenguaje ZF^+. Más exactamente, el axioma 6 afirma que existe un conjunto progresivo. La existencia de ω puede ser demostrada más tarde con ayuda del axioma de comprehensión.

Los axiomas no lógicos de ZF han sido elegidos de manera que en la teoría obtenida se puedan deducir todas las fórmulas cuya veracidad informal ya fue establecida en las secciones anteriores. Más exactamente, no se deben deducir, claro está, las fórmulas de ZF^+, sino sus traducciones al lenguaje ZF de acuerdo con las reglas dadas en la subsección 1.4.4: si en las secciones anteriores para cierta fórmula φ del lenguaje ZF^+ afirmamos que $.\varphi$, entonces ahora podemos demostrar que $ZF \vdash \varphi^0$. La realización de todas estas deducciones es una tarea engorrosa, pero es en realidad un ejercicio trivial de aplicación de las reglas de la deducción natural del cálculo de predicados. Aquí no nos detendremos en esto (esperamos que el lector se esfuerce por adquirir experiencia en la realización de deducciones formales).

El axioma de regularidad afirma que, en cierto sentido, todos los conjuntos se construyen a partir del conjunto vacío. Este axioma no se utiliza en la deducción de las afirmaciones matemáticas; nosotros tampoco lo hemos utilizado, pero él simplifica la estructura del universo de conjuntos y se incluye habitualmente en el grupo de axiomas no lógicos de ZF.

Una consecuencia del axioma de regularidad es la ausencia de conjuntos que pertenezcan a sí mismos, a saber, *no existen conjuntos tales que*

$$x \in x, \quad x \in y \wedge y \in x, \quad x \in y \wedge y \in z \wedge z \in x.$$

▶ Por ejemplo, supongamos que existen dos conjuntos x e y tales que $x \in y$ e $y \in x$. Consideremos el conjunto $Q = \{x, y\}$. Este conjunto no es vacío y, al mismo tiempo, no existe elemento de Q que no se interseque con Q, lo que contradice el axioma de regularidad. ◀

Análogamente, con ayuda del axioma de regularidad se puede demostrar que no existe una sucesión de conjuntos «decrecientes respecto a la pertenencia», es decir, no existe una función f, $\operatorname{dom} f = \omega$ tal que $f(n+1) \in f(n)$ para todo $n \in \omega$.

Una consecuencia del axioma de regularidad es el siguiente *principio de inducción por pertenencia*:

$$\forall x((\forall y \in x)\varphi(y) \supset \varphi(x)) \supset \forall x \varphi(x).$$

▶ Recordemos brevemente la demostración de este esquema. Supongamos que

$$\forall x((\forall y \in x)\varphi(y) \supset \varphi(x)),$$

y que se cumple lo contrario, es decir, que para cierto x $\neg\varphi(x)$. Consideremos una función f, $\operatorname{dom} f = \omega$ tal que $f(0) = \{x\}$ y $f(n+1) = \cup f(n)$. Sea $z = \bigcup_{n \in \omega} f(n)$.

Si $u \in z$, entonces $u \in f(n)$ para cierto n y, por tanto, $u \subseteq \subseteq f(n+1)$, es decir, $u \subseteq z$. De esta manera, $(\forall u \in z)(u \subseteq z)$ (esta propiedad se denomina *transitividad del conjunto* z). Además,

es evidente que $x \in z$, puesto que $x \in f(0)$. Supongamos que $z' = \{u \in z \mid \neg\varphi(u)\}$. El conjunto z' no es vacío, ya que $x \in z'$. Según el axioma de regularidad, existe $x' \in z'$ tal que $x' \cap z' = \varnothing$. Si $y \in x'$, entonces $y \notin z'$, es decir, según la definición de z', tenemos $y \notin z \vee \varphi(y)$. Pero el primer término de esta disyunción no se cumple, ya que $y \in x' \wedge x' \in z$ y el conjunto z es transitivo. Por tanto, $\varphi(y)$. Hemos demostrado $(\forall y \in x')\varphi(y)$. Según la suposición, de aquí se deduce $\varphi(x')$. Por otra parte, $x' \in z'$, lo que implica $\neg\varphi(x')$, y obtenemos una contradicción. ◄

A menudo, a la teoría ZF se incorpora el axioma de elección. Más exactamente, si con AC se denota la formulación exacta del axioma de elección, dada en la subsección 1.5.4, entonces a la teoría ZF, como nuevo axioma no lógico, se le debe añadir la fórmula AC^0. La teoría obtenida se denota con ZFC.

1.6.3 La teoría ZFC es excepcionalmente rica en lo que se refiere a sus posibilidades expresivas. Prácticamente todo teorema matemático demostrado puede ser escrito en el lenguaje ZF y deducida en la teoría ZFC. Además, las conocidas deducciones de las paradojas de la teoría de conjuntos no son válidas en ZFC.

En el sentido natural, la teoría ZF contiene todas las teorías axiomáticas formales que fueron consideradas en [11]. Démosle una forma más exacta a esta afirmación para el caso de la *aritmética formal* Ar, por ejemplo. Recordemos que el lenguaje Ar contiene un tipo de variables para los números naturales, una constante 0 y los símbolos de función $x + y$, $x \cdot y$, Sx para las correspondientes operaciones aritméticas. Como fórmulas atómicas se utiliza solamente la igualdad de términos $t = r$.

Representemos ahora los elementos del lenguaje Ar en el lenguaje ZF^+ y, a continuación, con ayuda del proceso de traducción estándar pasemos al lenguaje ZF. La constante 0 del lenguaje Ar se puede representar en forma del término cerrado $\varnothing$ del lenguaje ZF^+. Las variables para los números naturales del lenguaje Ar se representan en forma de variables subordinadas a la condición $x \in \omega$. Los símbolos de función del lenguaje Ar se expresan también mediante los términos respectivos de ZF^+; por ejemplo, al término Sx del lenguaje Ar le corresponde el término $x \cup \{x\}$ del lenguaje ZF^+.

De esta manera, a toda fórmula cerrada A del lenguaje Ar le corresponde cierta fórmula cerrada A' del lenguaje ZF^+ obtenida sustituyendo los elementos del lenguaje Ar por los elementos respectivos del lenguaje teórico-conjuntista. Finalmente, la fórmula obtenida A' se puede traducir al lenguaje ZF con ayuda del proceso de traducción indicado en la subsección 1.4.4. Seguidamente, no es difícil verificar que *si* A *es una fórmula cerrada de* Ar *y* $\mathrm{Ar} \vdash A$, *entonces* $\mathrm{ZF} \vdash A'$[0]. Esta afirmación se demuestra con ayuda de una voluminosa, pero en realidad trivial inducción respecto a la construcción de las deducciones en la teoría Ar.

La traducción obtenida es una *interpretación* natural de la teoría Ar en la teoría ZF. Esto le da un carácter más específico a la idea intuitivamente clara de que la teoría de conjuntos contiene en sí a la aritmética. De modo similar, se pueden construir en la teoría ZF interpretaciones de las restantes teorías que consideramos en [11]. En este sentido, la teoría ZF contiene a todas las demás teorías que ya hemos estudiado. Nótese que el concepto de interpretación es puramente sintáctico: se describe una transformación formal de las fórmulas de un lenguaje en fór-

mulas de otro, y se demuestra que esta transformación conserva la propiedad de una fórmula de ser deducible. No hay ninguna necesidad de analizar detalladamente la semántica de las fórmulas del lenguaje Ar o del lenguaje ZF.

Esto nos da la posibilidad de demostrar de manera puramente sintáctica la *consistencia relativa* de las teorías. Por ejemplo, si la teoría ZF es consistente, entonces también lo es la teoría Ar. En efecto, si Ar es contradictoria, entonces existe una sentencia A tal que $\mathrm{Ar} \vdash A \wedge \neg A$. Pero entonces $\mathrm{ZF} \vdash A'^0 \wedge \neg A'^0$, lo que significa que también la teoría ZF resulta contradictoria. Análogamente, de la consistencia de ZF se deduce la consistencia de las otras teorías consideradas por nosotros. Desde el punto de vista de los fundamentos de la matemática, es importante que el problema de la consistencia de las demás teorías se reduce a la consistencia de ZF sin recurrir a la semántica de estas teorías y puede ser formulado en una teoría muy modesta, por ejemplo, en Ar.

1.6.4 Ahora podemos dar una formulación más exacta de la afirmación de que el axioma de elección y la hipótesis del continuo son independientes de la teoría de conjuntos.

Teorema. *El axioma de elección (es decir, la fórmula* AC^0*) no depende de la teoría* ZF.

Teorema. *La hipótesis del continuo no depende de la teoría* ZFC.

Estos admirables resultados fueron obtenidos por K. Gödel y P. Cohen. A saber, en 1939 Gödel demostró la compatibilidad del axioma de elección y la hipótesis del continuo con la teoría ZF, para lo que construyó una excelente interpretación de ZFC con la hipótesis del continuo en la teoría ZF. En 1963

Cohen demostró la compatibilidad de la negación del axioma de elección con ZF y la compatibilidad de la negación de la hipótesis del continuo con ZFC, indicando también algunas interpretaciones concretas. En la actualidad ha sido demostrado que muchas afirmaciones interesantes de la teoría de conjuntos son independientes de ZF y de ZFC . Las demostraciones de estos resultados se pueden hallar en [5, 12, 13].

Analicemos nuevamente, en relación con los teoremas mencionados, la pregunta «ingenua» de si se puede considerar, por ejemplo, la hipótesis del continuo H como una afirmación verdadera y en qué sentido concretamente? De los resultados mencionados se deduce que *si la teoría* ZF *es consistente*, entonces en ZFC no se puede deducir la fórmula H ni la fórmula $\neg H$. La teoría ZFC contiene todos los medios de demostración de afirmaciones matemáticas utilizados tradicionalmente; por tanto, H no puede ser demostrada ni refutada con ayuda de *medios matemáticos tradicionales*. El conjunto de medios matemáticos tradicionales de demostración de ZFC es incompleto.

¿Será posible proponer teorías más potentes en las que el problema sobre H pueda ser resuelto de una manera determinada? La respuesta es trivial. Por supuesto, esto es posible. De los resultados indicados anteriormente se deduce que si ZF es consistente, entonces la teoría ZFC + H, obtenida añadiendo la afirmación H a la teoría ZFC como nuevo axioma no lógico, también es consistente. La teoría ZFC + $\neg H$ también es consistente. De esta manera, el problema consiste en cuál de estas dos teorías se prefiere y por qué se prefiere. En la actualidad, no se tienen motivos suficientes para indicar una u otra de estas teorías como «la que en realidad es correcta»; los matemáticos

prácticos tratan de no utilizar ni H ni $\neg H$ en sus razonamientos. A propósito, algunos matemáticos reconocidos, como por ejemplo P. Cohen [2, cap. IV, sec. 13], consideran que sería más natural considerar que la hipótesis del continuo es una afirmación falsa.

El problema también puede ser abordado desde otro punto de vista. En la secciones 1.2–1.5 considerábamos cierta estructura imaginaria $\mathcal{M}_0$, formada por objetos que satisfacían los axiomas de ZF. Ahora bien, ¿es verdadera la afirmación H en $\mathcal{M}_0$ o no? Nótese que lo único que exigíamos de $\mathcal{M}_0$ era que en ella se cumplieran los axiomas de ZF. No existen motivos para afirmar que todas estas estructuras son isomorfas; es absolutamente posible que en un modelo de ZFC sea verdadera H, mientras que en otro sea verdadera la afirmación $\neg H$. Precisamente ésta es la situación. Si ZF es consistente, entonces es consistente cada una de las teorías ZFC$+H$ y ZFC$+\neg H$. De acuerdo con el conocido teorema de completitud de Gödel, cada una de estas teorías tiene un modelo y cualquiera de estos dos modelos puede ser tomado como estructura $\mathcal{M}_0$. Desde el punto de vista de los fundamentos de la matemática es útil señalar que la propia demostración del teorema de completitud de Gödel en el caso considerado no necesita de las potentes ideas teórico-conjuntistas contenidas en los axiomas de ZF; esta demostración puede ser formalizada de una manera natural en el marco de, por ejemplo, la aritmética de segundo orden Ar2 (véase [9]).

1.6.5 Discutamos otro problema relacionado con la teoría ZF, el cual a menudo es motivo de confusión. Del teorema de completitud de Gödel se deduce, en particular, que si la teoría ZF es consistente, entonces ella admite un modelo numerable M. ¿Cómo concuerda esta circunstancia con el hecho evidente de que

en ZF la existencia de conjuntos no numerables es deducible? (Por ejemplo, el conjunto $P\omega$ no es numerable).

Todo modelo M de la teoría ZF tiene la forma $\langle X, \varepsilon \rangle$, donde X es un conjunto no vacío de objetos y ε es una relación, $\varepsilon \subseteq X \times X$, que interpreta la pertenencia $\in$ en el conjunto X. En esta interpretación, todos los axiomas de ZF son verdaderos.

La fórmula $\exists x(x = P\omega)$ es verdadera en M; por tanto, existe un objeto $a \in X$ tal que $M \models (a = P\omega)$. Para mayor brevedad, aquí y en lo sucesivo escribimos fórmulas de ZF^+, y no de ZF. Por supuesto, se sobrentiende que ellas deben ser traducidas al lenguaje ZF con ayuda del proceso de traducción estándar de la subsección 1.4.4.

La fórmula que afirma que x es numerable tiene la forma

$$\mathrm{Count}(x) \leftrightharpoons \exists f((1-1)(f) \wedge \mathrm{dom}\, f = x \wedge \mathrm{rng}\, f = \omega).$$

En ZF es deducible que $P\omega$ es un conjunto no numerable, lo que significa que este hecho es verdadero en M, es decir,

$$M \models \neg\mathrm{Count}(a).$$

Según la definición de veracidad en una estructura, esto último significa que no existe un objeto $b \in X$ tal que

$$M \models (1-1)(b) \wedge \mathrm{dom}\, b = a \wedge \mathrm{rng}\, b = \omega,$$

es decir, **entre los elementos** de X no existe un objeto b tal que en M **sea verdadero** que b es una función biunívoca con dominio a e imagen ω. En este caso, carece de importancia cuál es la naturaleza de a; por ejemplo, desde un punto de vista externo, a puede ser un conjunto numerable, de modo que existe una biyección de a sobre ω. Lo que sucede es que entre los elementos

de X, desde el punto de vista del modelo M, no existe la biyección necesaria. La veracidad de las afirmaciones depende del modelo en el que estas afirmaciones son consideradas. Un mismo objeto que es elemento de diferentes modelos puede poseer propiedades diferentes en estos modelos.

El fenómeno indicado habitualmente es denominado *paradoja de Skolem*. Por supuesto, se debe tener en cuenta que aquí en realidad no estamos en presencia de una paradoja en el sentido propio de esta palabra. En este caso existe, posiblemente, cierta confusión de conceptos que desorienta a quien no es especialista.

Un malentendido similar a menudo surge en lo relacionado con la categoricidad de ciertas estructuras, por ejemplo, del conjunto de los números naturales.

Con ayuda de razonamientos bien conocidos de la teoría de números, en ZF se puede demostrar que todas las *estructuras de Peano* (es decir, estructuras de la forma $\langle \omega^*, 0^*, S^* \rangle$, donde ω^* es un conjunto, $0^* \in \omega^*$ y S^* es la operación $S^* : \omega^* \to \omega^*$, que satisfacen los *axiomas de Peano*; véase la subsección 1.4.1) son isomorfas, es decir, las estructuras de Peano representan un conjunto de números naturales único salvo isomorfismos. En esto precisamente consiste la propiedad de *categoricidad* del conjunto de los números naturales.

No obstante, en **diferentes modelos** los conjuntos de números naturales pueden no ser isomorfos. Consideremos dos modelos de la teoría ZF: $M_1 = \langle X_1, \varepsilon_1 \rangle$ y $M_2 = \langle X_2, \varepsilon_2 \rangle$. Tenemos $\mathrm{ZF} \vdash \exists x(x = \omega)$, de modo que existen objetos $\omega_1 \in X_1$ y $\omega_2 \in X_2$ tales que $M_1 \models \omega_1 = \omega$ y $M_2 \models \omega_2 = \omega$. En cada uno de estos modelos podemos considerar también un «conjunto de números naturales»:

$$N_1 = \{a \in X_1 \mid M_1 \models a\varepsilon_1\omega_1\}, \quad N_2 = \{a \in X_2 \mid M_2 \models a\varepsilon_2\omega_2\}.$$

En cada uno de los modelos M_i existe su propio objeto O_i y su propia operación S_i de adición de la unidad. Pero la estructura $\langle N_i, O_i, S_i\rangle$ no necesariamente satisface los axiomas de Peano desde un punto de vista externo. Sólo es necesario que en el **modelo** M_i sean verdaderas las fórmulas correspondientes. Las estructuras $\langle N_i, O_i, S_i\rangle$ pueden no ser isomorfas al conjunto de los números naturales comprendido informalmente y no ser isomorfas entre sí. Una estructura para la cual en un modelo es verdad que ella es una estructura de Peano puede no serlo desde un punto de vista externo. Más adelante veremos que si la teoría ZF es consistente, entonces ella necesariamente tiene modelos que no son isomorfos al conjunto de los números naturales.

1.6.6 En las secciones 1.2–1.4, consideramos los principios de ZF como informalmente verdaderos, que se cumplen en cierta estructura $\mathcal{M}_0$, y tratamos de demostrar que los conceptos matemáticos fundamentales pueden ser expresados en el lenguaje ZF, y muchas de las afirmaciones matemáticas tienen lugar en $\mathcal{M}_0$. En este caso no se establecieron los medios de demostración.

Seguidamente, definimos la teoría axiomática formal ZF, en la cual existe la posibilidad de obtener los resultados anteriores en forma de deducciones exactas. Para la construcción de deducciones en la teoría ZF, no es necesario analizar detalladamente la semántica del lenguaje ZF, pero para estudiar la *propia* teoría ZF, por ejemplo, para obtener resultados relacionados con la independencia, también es necesaria desde luego cierta matemática. Esta matemática se utilizará nuevamente de una manera no formalizada. En relación con la teoría estudiada, ella es deno-

minada *metamatemática*. En general, un investigador puede estudiar la metamatemática y también tratar de formalizarla.

¿Cuál debe ser la metamatemática de una teoría? Desde el punto de vista de los fundamentos de la matemática existe la tendencia a hacer la metamatemática lo más pobre que se pueda con el fin de que los razonamientos en ella sean lo más sencillos y convincentes que sea posible. Así pues, se puede decir que los resultados relacionados con una teoría muy compleja han sido obtenidos con ayuda de métodos muy convincentes de demostración. Por ejemplo, los resultados concernientes a la independencia del axioma de elección y la hipótesis del continuo pueden ser naturalmente formalizados en el marco de la aritmética Ar de manera que en estas demostraciones no figure el concepto de conjunto. Muchos otros resultados de la lógica matemática pueden ser obtenidos utilizando la teoría de conjuntos de forma limitada, por ejemplo, en el marco de la aritmética de segundo orden.

Por otra parte, fuera del marco de los fundamentos de la matemática, la lógica matemática puede ser desarrollada como una disciplina matemática habitual, como la topología o la teoría de funciones. En esta situación no hay razones para restringir de manera alguna la metamatemática. Se puede, por ejemplo, tomar la *propia teoría* ZF como metamatemática. Justamente de tal manera proceden en muchas investigaciones de teorías de modelos, de análisis no estándar, etcétera. En este sentido, la teoría ZF interviene en el papel de «universo de los conjuntos» para todos los matemáticos.

Se debe subrayar que la teoría ZF no es la única posibilidad para el desarrollo de la matemática sobre una base exacta.

Su amplia utilización se debe a las considerables conveniencias formales que ella ofrece, y también en parte a la tradición histórica. En la actualidad, en la lógica han sido elaborados numerosos métodos interesantes y muy prometedores para el desarrollo de las teorías matemáticas, los cuales no se basan en el concepto de conjunto. Uno de ellos es el *constructivismo* en la matemática, que ha obtenido un gran impulso en nuestro país. Existen otros sistemas teórico-conjuntistas que pueden competir exitosamente con la teoría ZF. Entre ellos podemos mencionar, en primer lugar, la *teoría de tipos* de Russell y Whitehead, así como la *teoría de conjuntos de Quine.*

De acuerdo con un conocido teorema de Gödel, la consistencia de ZF no puede demostrada utilizando los medios de ZF, es decir, no puede ser demostrada con ayuda de los medios matemáticos tradicionales. Por tanto, si deseamos investigar la consistencia de potentes teorías como ésta, nos vemos en la necesidad de hallar medios matemáticos, por una parte, suficientemente convincentes en uno u otro sentido y, por otra parte, que superen los marcos de la práctica matemática tradicional.

El análisis detallado de muchos de los problemas tratados aquí pueden ser hallados por el lector en [5].

1.6.7. Hagamos algunas observaciones relacionadas con la utilización del método axiomático en la lógica matemática. El término «método axiomático» se utiliza en diferentes sentidos, lo que a veces provoca malentendidos.

Ante todo, tenemos el *método axiomático informal.* Éste se utiliza cuando se estudia un género de estructuras que satisfacen una misma lista de propiedades. Por ejemplo, los grupos forman un género de estructuras, otro género de estructuras

lo constituyen los anillos, un tercer género de estructuras está formado por las estructuras de Peano, etcétera. Como *axiomas* se toman las condiciones concretas que deben ser satisfechas por toda estructura del género estudiado. Estas condiciones se entienden informalmente y se escriben en un lenguaje matemático de trabajo, por ejemplo, en ruso o en español. A menudo los axiomas de un género de estructuras se escriben en un lenguaje lógico-matemático exacto, pero son entendidos informalmente, como afirmaciones sobre estructuras; para algunas estructuras estos axiomas pueden ser verdaderos, para otras, falsos.

La forma de entender estos axiomas depende de la metamatemática aceptada. Sobre todo, esto es esencial en los casos cuando en las formulaciones de los axiomas, aparte de los objetos de la estructura, figuran otros objetos, por ejemplo, conjuntos. Éstos son los denominados *axiomas no elementales*.

Por ejemplo, entre los axiomas de la estructura de Peano $\langle \omega, O, S \rangle$, se tiene el siguiente: para todo subconjunto $x \subseteq \omega$, se cumple el principio de inducción completa $O \in x \wedge (\forall y \in x)(Sy \in x) \supset (\forall y \in \omega)(y \in x)$. Para comprender esta afirmación se debe comprender qué es un subconjunto de un conjunto dado y cuáles son las reglas para tratar con estos subconjuntos. Si como metamatemática tomamos los principios de ZF comprendidos informalmente (como se hace en la matemática práctica), entonces el significado de este axioma se aclara en cierta medida, se pueden obtener consecuencias informales a partir de él, por ejemplo, se puede demostrar que todas las estructuras de Peano son isomorfas. Podemos imaginar esta situación como si se hubiera fijado cierta estructura $\mathcal{U}_0$ que concuerda con los principios de ZF. Sólo de $\mathcal{U}_0$ tomamos los objetos de la inves-

tigación matemática. Después de esto se puede demostrar que todas las estructuras de Peano en $\mathcal{M}_0$ son isomorfas entre sí.

Una situación diferente surge cuando las teorías se estudian mediante el *método axiomático formal*. Los aspectos fundamentales relacionados con las estructuras estudiadas se presentan en forma de una teoría axiomática formal T. Los nuevos resultados sobre la teoría T se obtienen (al menos, en principio) con ayuda del aparato de deducibilidad formal. En este caso, la semántica inicial de T no tiene importancia alguna, y no hay necesidad de referirse a los modelos de la teoría T. Es más, entre los modelos de la teoría axiomática formal T, puede haber algunos que no fueron incluidos entre los modelos que inicialmente se habían supuesto como tales. Por ejemplo, si la teoría ZF es consistente, entonces entre sus modelos existe uno numerable.

Por *axiomas* de la teoría T entendemos ahora sus axiomas no lógicos, es decir, fórmulas de tipo especial; el significado de estos axiomas no es, en general, importante para la formulación de la teoría T. Pero, por supuesto, si nuestra intención es deducir en T resultados no triviales, la teoría T debe ser dotada de una lista suficientemente rica de axiomas. Por ejemplo, si estudiamos las estructuras de Peano y escribimos el principio de inducción en el lenguaje ZF, entonces deberemos añadir a esta teoría los axiomas que determinan las propiedades de los conjuntos

lo constituyen los anillos, un tercer género de estructuras está formado por las estructuras de Peano, etcétera. Como *axiomas* se toman las condiciones concretas que deben ser satisfechas por toda estructura del género estudiado. Estas condiciones se entienden informalmente y se escriben en un lenguaje matemático de trabajo, por ejemplo, en ruso o en español. A menudo los axiomas de un género de estructuras se escriben en un lenguaje lógico-matemático exacto, pero son entendidos informalmente, como afirmaciones sobre estructuras; para algunas estructuras estos axiomas pueden ser verdaderos, para otras, falsos.

La forma de entender estos axiomas depende de la metamatemática aceptada. Sobre todo, esto es esencial en los casos cuando en las formulaciones de los axiomas, aparte de los objetos de la estructura, figuran otros objetos, por ejemplo, conjuntos. Éstos son los denominados *axiomas no elementales*.

Por ejemplo, entre los axiomas de la estructura de Peano $\langle \omega, O, S \rangle$, se tiene el siguiente: para todo subconjunto $x \subseteq \omega$, se cumple el principio de inducción completa $O \in x \wedge (\forall y \in x)(Sy \in x) \supset (\forall y \in \omega)(y \in x)$. Para comprender esta afirmación se debe comprender qué es un subconjunto de un conjunto dado y cuáles son las reglas para tratar con estos subconjuntos. Si como metamatemática tomamos los principios de ZF comprendidos informalmente (como se hace en la matemática práctica), entonces el significado de este axioma se aclara en cierta medida, se pueden obtener consecuencias informales a partir de él, por ejemplo, se puede demostrar que todas las estructuras de Peano son isomorfas. Podemos imaginar esta situación como si se hubiera fijado cierta estructura $\mathcal{U}_0$ que concuerda con los principios de ZF. Sólo de $\mathcal{U}_0$ tomamos los objetos de la inves-

tigación matemática. Después de esto se puede demostrar que todas las estructuras de Peano en $\mathcal{M}_0$ son isomorfas entre sí.

Una situación diferente surge cuando las teorías se estudian mediante el *método axiomático formal*. Los aspectos fundamentales relacionados con las estructuras estudiadas se presentan en forma de una teoría axiomática formal T. Los nuevos resultados sobre la teoría T se obtienen (al menos, en principio) con ayuda del aparato de deducibilidad formal. En este caso, la semántica inicial de T no tiene importancia alguna, y no hay necesidad de referirse a los modelos de la teoría T. Es más, entre los modelos de la teoría axiomática formal T, puede haber algunos que no fueron incluidos entre los modelos que inicialmente se habían supuesto como tales. Por ejemplo, si la teoría ZF es consistente, entonces entre sus modelos existe uno numerable.

Por *axiomas* de la teoría T entendemos ahora sus axiomas no lógicos, es decir, fórmulas de tipo especial; el significado de estos axiomas no es, en general, importante para la formulación de la teoría T. Pero, por supuesto, si nuestra intención es deducir en T resultados no triviales, la teoría T debe ser dotada de una lista suficientemente rica de axiomas. Por ejemplo, si estudiamos las estructuras de Peano y escribimos el principio de inducción en el lenguaje ZF, entonces deberemos añadir a esta teoría los axiomas que determinan las propiedades de los conjuntos

CAPÍTULO

2

ELEMENTOS DE TEORÍA DE ALGORITMOS

2.1. Máquinas de Turing 107
2.2. Tesis de Church 123
2.3. Conjuntos y predicados recursivos y recursivamente enumerables 126
2.4. Funciones recursivas primitivas. Numeración de Gödel. Aritmética con términos recursivos primitivos 140
2.5. Algunos teoremas de la teoría general de algoritmos 155

2.1 Máquinas de Turing

2.1.1 La importancia de los algoritmos en la matemática es bien conocida. Sin entrar en detalles, podemos decir que un *algoritmo* es una prescripción exacta en correspondencia con la cual para cualquier objeto de entrada perteneciente a una clase dada de objetos de entrada se pueden obtener de manera efectiva objetos de salida. Por ejemplo, el algoritmo de la multiplicación habitual de números racionales decimales permite para dos notaciones decimales obtener una tercera de acuerdo con una prescripción que es bien conocida por todos. También son algoritmos el esquema de Horner, para el cálculo de los valores de un polinomio, el algoritmo de Euclides, para hallar la medida máxima común de dos segmentos, el algoritmo de multiplicación de dos matrices cuadradas, etcétera.

Para someter el concepto de algoritmo a un análisis exacto, es necesario reducir en cierta medida la clase de algoritmos que se desea considerar. Ante todo, supondremos que los algoritmos son *prescripciones discretas* semejantes a los programas de computadora, y no similares a las computadoras analógicas o gráficas. Una pres-

cripción debe contener instrucciones para la ejecución de un número finito de pasos elementales bien distinguibles. Por eso, también los datos de entrada de los algoritmos estudiados deben ser objetos discretos, *constructivos*, como los números naturales, los números racionales, las matrices de elementos enteros, etcétera. No pueden ser datos de entrada, por ejemplo, segmentos de recta cualesquiera, números reales arbitrarios, puesto que estos objetos no pueden ser, en el caso general, definidos de manera finita.

Señalemos que en la matemática un papel muy importante es desempeñado por prescripciones exactas destinadas al procesamiento de objetos no constructivos. Los algoritmos de este tipo también se estudian en la lógica matemática, pero para el estudio inicial nos limitaremos a la clase más importante, a los dispositivos discretos puros. De esta manera, el algoritmo de multiplicación de los números racionales decimales, el esquema de Horner para polinomios con coeficientes racionales y el algoritmo de multiplicación de matrices cuadradas con elementos naturales son algoritmos de esta clase. El algoritmo de búsqueda de la medida máxima común de dos segmentos arbitrarios quedará por ahora fuera de nuestro análisis.

El concepto de objeto constructivo sigue siendo todavía muy impreciso, pero sería razonable suponer que los objetos constructivos que nos interesan se pueden codificar efectivamente en forma de palabras sobre cierto alfabeto. De este modo, se puede considerar que con cada algoritmo A está relacionado un alfabeto Σ, denominado *alfabeto externo* de A, y el algoritmo recibe en la entrada palabras sobre el alfabeto Σ y proporciona como resultados también palabras sobre el alfabeto Σ. Nosotros sólo estudiaremos los algoritmos *de palabras*.

Un algoritmo es una construcción íntegra en cuya entrada se puede introducir cualquier palabra de una lista de palabras de entrada, que en general puede ser infinita. En esto consiste la *propiedad de generalidad* de un algoritmo. Por conveniencia, consideremos que en la entrada del algoritmo A se puede introducir *cualquier* palabra sobre el alfabeto externo Σ. Una vez obtenida la palabra de entrada, se debe aplicar a ella la prescripción del algoritmo A paso por paso. Es posible que la ejecución de los pasos del algoritmo se detenga y se obtenga una palabra de salida como resultado. También puede ocurrir que la prescripción origine una sucesión infinita de operaciones elementales; en este caso, el algoritmo A no está definido en la palabra de entrada dada.

En lo sucesivo, consideraremos que los algoritmos estudiados poseen *propiedad de determinación*: cada paso elemental está determinado unívocamente por la situación anterior. Los algoritmos que analizaremos no tienen mecanismos aleatorios o probabilísticos incorporados. En particular, si los cálculos de un algoritmo se efectúan dos veces sobre una misma entrada, los resultados serán iguales.

Finalmente, los algoritmos que consideraremos deben poseer *propiedad de aislamiento*, es decir, la ejecución de los cálculos está definida sólo por la prescripción, y no es necesario incorporar, aparte de la palabra de entrada, procesos o dispositivos de cálculo externos.

Se puede suponer que todas las operaciones que pueden ser producidas por un algoritmo del tipo indicado se pueden descomponer en varios pasos canónicos elementales. Este análisis determinó la creación del concepto de máquina de cálculo por Turing en 1936, que posteriormente recibiría su nombre.

2.1.2 Pasemos ahora a las definiciones exactas. Recordemos que, por definición, un *alfabeto* es un conjunto finito no vacío de símbolos. Los elementos de un alfabeto son denominados *letras* del alfabeto. Una *palabra* Σ es una sucesión finita (posiblemente vacía) de letras del alfabeto. Una palabra sobre un alfabeto Σ tiene, por consiguiente, la forma $a_0a_1 \dots a_n$, donde $a_i \in \Sigma$. El conjunto de todas las palabras sobre el alfabeto Σ se denota con Σ^*.

La operación principal que se realiza con las palabras es la *concatenación de palabras*: si tenemos una palabra A de la forma $a_0a_1 \dots a_n$ y una palabra B de la forma $b_0b_1 \dots b_m$, entonces se puede formar una nueva palabra AB de la forma $a_0a_1 \dots a_nb_0 \dots b_m$, llamada *concatenación* de las palabras A y B.

La palabra vacía se denota con Λ. Evidentemente,

$$A\Lambda = \Lambda A = A.$$

Tomemos dos alfabetos Σ y S. Llamemos *alfabeto externo* al alfabeto Σ y *alfabeto interno* o *alfabeto de estados* al alfabeto S. Supongamos que los símbolos $\rightarrow$, R, L no figuran ni en Σ ni en S.

Denominaremos *instrucción* a toda palabra de una de las tres formas siguientes:

$$qa \rightarrow rb,$$

$$qa \rightarrow rbR,$$

$$qa \rightarrow rbL,$$

donde $q, r \in S$; $a, b \in \Sigma$. Las instrucciones, de la misma manera que las fórmulas de un lenguajes, se pueden leer en cualquier lenguaje natural. La instrucción de la primera forma se puede leer así: «si estamos en el estado q y leemos la letra a,

debemos pasar al estado r y escribir la letra b». La instrucción de la segunda forma puede leerse así: «si estamos en el estado q y leemos la letra a, debemos pasar al estado r, escribir la letra b y desplazarnos a la derecha». La tercera instrucción se lee de la misma forma que la segunda, pero al final se debe leer «...y desplazarnos a la izquierda».

Por definición, una *lista de instrucciones* o *programa* (sobre los alfabetos Σ, S) es una sucesión finita de instrucciones.

Supongamos ahora que tenemos dos alfabetos, Σ y S, dos letras q_0 y $q_1 \in S$ y una letra $a_0 \in \Sigma$. La letra q_0 se denomina *estado inicial*; la letra q_1, *estado final*; y la letra a_0, *blanco* (en otra terminología, *vacío*).

El alfabeto $S \times \Sigma$ se denomina *alfabeto de letras leídas*. De la letra $\langle q, a \rangle \in S \times \Sigma$ decimos que «a *se lee* en el estado q».

Se denomina *configuración de cinta* (o *palabra de máquina*) a la palabra sobre el alfabeto $\Sigma \cup (S \times \Sigma)$ que contiene exactamente una aparición de la letra leída. De esta manera, una configuración siempre tiene la forma $A\langle q, a\rangle B$, donde $A, B \in \Sigma^*$ y la letra a se lee en el estado q.

Una configuración se denomina *inicial* si ella tiene la forma $\langle q_0, a\rangle B$. Aquí, q_0 es el estado inicial, y la palabra A en el caso dado es vacía. Una configuración se denomina *final* si tiene la forma $A\langle q_1, a\rangle B$, es decir, la letra es leída en el estado final.

Supongamos ahora que K_1 y K_2 son configuraciones, y k es una instrucción. Definamos qué significa que la instrucción k *transforma* la configuración K_1 en la configuración K_2; esto se escribe simbólicamente de la siguiente manera

$$k : K_1 \triangleright K_2.$$

Más exactamente, supongamos que K_1 tiene la forma $A\langle q, a\rangle B$. Si el miembro izquierdo de la instrucción k no tiene la forma qa, entonces $k : K_1 \triangleright K_2$ se considera falso automáticamente (la instrucción k es *inaplicable* a la configuración K_1). Supongamos que el primer miembro de la instrucción k tiene la forma qa. Analicemos tres casos, en dependencia de la estructura de la instrucción k:

1) k es $qa \to rb$. En este caso, $k : K_1 \triangleright K_2 \Leftrightarrow K_2$ tiene la forma $A\langle r, b\rangle B$.
2) k es $qa \to rbR$. Aquí debemos considerar dos casos:
   a) La palabra B no es vacía, $B = cB'$. Entonces,
   $$k : K_1 \triangleright K_2 \Leftrightarrow K_2 \quad \text{es} \quad Ab\langle r, c\rangle B'.$$
   b) La palabra B es vacía. Entonces,
   $$k : K_1 \triangleright K_2 \Leftrightarrow K_2 \quad \text{es} \quad Ab\langle r, a_0\rangle.$$
3) k es $qa \to rbL$. Aquí también debemos considerar dos casos:
   a) La palabra A no es vacía, $A = A'c$. Entonces,
   $$k : K_1 \triangleright K_2 \Leftrightarrow K_2 \quad \text{es} \quad A'\langle r, c\rangle bB;$$
   b) La palabra A es vacía. Entonces,
   $$k : K_1 \triangleright K_2 \Leftrightarrow K_2 \quad \text{es} \quad \langle r, a_0\rangle bB.$$

Es obvio que si $k : K_1 \triangleright K_2$, entonces la configuración K_2 está unívocamente definida por la instrucción k y la configuración K_1.

Podemos concebir una configuración como una palabra escrita en una cinta dividida en celdas, en cada una de las cuales está escrita una letra del alfabeto Σ. Sobre una de las letras está escrito un estado; ésta es la letra que la máquina lee.

Transformar K_1 en K_2 mediante la instrucción k significa «ejecutar» la instrucción k, hacer lo que «ella exige». Después de la ejecución de la instrucción, se lee otra letra, que puede encontrarse a la izquierda o a la derecha de la inicial. Si en este caso es necesario salir de los límites de la cinta a la izquierda y a la derecha, entonces la ejecución de la instrucción estipula automáticamente la adición de una nueva celda, en la que se considera escrita la letra a_0, una «celda vacía», un «blanco».

Por definición, una *máquina de Turing* es una 6-tupla

$$M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle,$$

donde

Σ — alfabeto externo, q_0 — estado inicial,

S — alfabeto interno, q_1 — estado final,

Π — programa de la máquina, a_0 — blanco.

Las instrucciones del programa Π de la máquina M se escriben por lo general verticalmente, numeradas de arriba hacia abajo:

$$k_1$$
$$k_2$$
$$\vdots$$
$$k_m.$$

Diremos que una máquina M *transforma* la configuración K_1 en la configuración K_2 (en este caso, escribiremos $M : K_1 \triangleright K_2$) si

1) existe una instrucción k_i del programa de la máquina M tal que $k_i : K_1 \triangleright K_2$, y
2) para todo $j < i$ no existe una configuración K_3 tal que $k_i : K_1 \triangleright K_3$.

De esta manera, si $M : K_1 \triangleright K_2$, entonces la configuración K_2 está definida unívocamente por M y K_1. Por supuesto, es posible que cierta configuración K_1 no es transformada por la máquina M en ninguna configuración K_2.

El *protocolo de cálculo* de una máquina de Turing M es una sucesión (finita o infinita) de configuraciones

$$K_0, K_1, \ldots, K_n, \ldots$$

tal que

1) K_0 es la configuración inicial;
2) $M : K_i \triangleright K_{i+1}$;
3) si la configuración K_i figura en el protocolo $M : K_i \triangleright K_{i+1}$ y K_i no es una configuración final, entonces K_{i+1} también figura en el protocolo de cálculo (es decir, el protocolo no termina con la configuración K_i si los cálculos pueden ser continuados);
4) el protocolo de cálculo puede contener no más de una configuración final, y si el protocolo realmente contiene una configuración final, entonces este protocolo es finito y la configuración final es su último término.

Escribiremos $M\lfloor K_0 \rfloor = K_n$ si K_0 es la configuración inicial, K_n es la configuración final y existe un protocolo de cálculo

de la máquina M que comienza con K_0 y termina con K_n. Para M y K_0 dados, el protocolo de cálculo (si él existe) puede ser sólo uno, de modo que el resultado de los cálculos K_n (si él existe) está determinado unívocamente. Diremos que M está *definida* para K_0 si la configuración final respectiva K_n existe.

Existen dos motivos que pueden hacer que una máquina no esté definida para una configuración inicial K_0: o bien durante el proceso de construcción del protocolo de cálculo llegamos a una configuración a la que no se le puede aplicar ninguna instrucción de la máquina, o bien el protocolo de cálculo es infinito y no conduce a una configuración final. Por supuesto, es imposible para una máquina dada M y una configuración K_0 decir de antemano si M está definida para K_0, y si no lo está, determinar cuál de los casos mencionados anteriormente es el que tiene lugar.

Si se tiene una palabra $A \in \Sigma^*$, entonces para ella se puede preparar de manera estándar cierta configuración inicial A^0 para la máquina M o, como se dice, introducir la palabra A en la entrada de la máquina M. A saber, si A no es vacía, $A = aA'$, entonces se debe tomar $A^0 = \langle q_0, a\rangle A'$. Si A es vacía, entonces $A^0 = \langle q_0, a_0\rangle$. En resumen, se debe «obligar» a la máquina a leer la primera letra A en el estado inicial. Si en A no hay letras entonces, por supuesto, se debe obligar a la máquina a leer una celda vacía de la máquina.

Por otra parte, para cualquier configuración K de la máquina podemos preparar cierta palabra $K^1 \in \Sigma^*$. Diremos que la palabra K^1 está escrita en la cinta en la configuración K. Para esto se debe proceder de la siguiente manera:

1) en primer lugar, se debe eliminar el estado de la letra que se lee, es decir, sustituir la letra leída $\langle q, a\rangle$ en la configu-

ración K por la letra habitual a, de modo que se obtiene cierta palabra A sobre el alfabeto Σ;

2) a continuación, en la palabra A se deben borrar todas las celdas vacías dispuestas una tras otra, a la izquierda y a la derecha, es decir, si $A = BCD$, donde B y D están formadas sólo por la letra a_0, y la palabra C no comienza y no termina con la letra a_0, entonces como K^1 se debe dejar la palabra C.

Puede resultar que K^1 es una palabra vacía (si en la configuración K figuraba sólo la letra a_0 de Σ).

2.1.3 De esta manera, una máquina de Turing M con alfabeto externo Σ genera una función que procesa palabras sobre el alfabeto Σ para obtener palabras sobre el mismo alfabeto Σ. A saber, para $A, B \in \Sigma^*$, $M(A) = B \Leftrightarrow$ existen dos configuraciones K_0 y K_n tales que $M\lfloor K_0 \rfloor = K_n$ y $(K_0)^0 = A$, $(K_n)^1 = B$. En resumen, si en la entrada se introduce la palabra A, entonces el correspondiente protocolo de cálculo finaliza y en la cinta resulta escrita la palabra B.

Nótese que la función M puede no estar definida en todas las palabras sobre el alfabeto Σ. Diremos que una máquina M *está definida* en la palabra A (en este caso escribiremos $!M(A)$) si M está definida en la configuración inicial A^0.

Las máquinas de Turing pueden ser imaginadas como un tipo determinado de computadoras que procesan palabras sobre alfabetos e imitan el funcionamiento de computadoras reales o el trabajo de una persona que calcula. La máquina funciona con una cinta dividida en celdas. En todo instante se considera

sólo un tramo finito de esta cinta, pero a medida que va siendo necesario la cinta se prolonga infinitamente hacia ambos lados.

La máquina puede escribir en la cinta algunas letras del alfabeto y leer en cada instante sólo una celda de la cinta. Las operaciones de la máquina son realizadas por pasos que están determinados unívocamente por el estado de la máquina en el momento dado, por el contenido de la celda leída y por el programa de la máquina. La máquina se detiene cuando alcanza un estado final. Puede ocurrir que, al iniciar su trabajo en cierta palabra, la máquina nunca se detenga.

2.1.4 Definamos ahora qué significa que una función es computable con ayuda de una máquina de Turing.

Recordemos algunas notaciones. Si $X_1, \ldots, X_k$ son conjuntos, entonces con $X_1 \times \ldots \times X_k$ denotamos el producto cartesiano de estos conjuntos, es decir, el conjunto de todas las k-tuplas ordenadas $\langle x_1, \ldots, x_k, \rangle$, donde $x_1 \in X_1, \ldots, x_k \in X_k$. Si X e Y son conjuntos, entonces con $X \to Y$ denotamos el conjunto de todas las funciones con dominio X que toman valores en el conjunto Y. Tradicionalmente, en lugar de $f \in (X \to Y)$ se escribe $f : X \to Y$. Una función de k argumentos es una función de la forma $f : X_1 \times \ldots \times X_k \to Y$, es decir, $f(\langle x_1, \ldots, x_k \rangle) \in Y$. Por tradición, la notación $f(\langle x_1, \ldots, x_k \rangle)$ se simplifica y se escribe $f(x_1, \ldots, x_k)$.

Denotemos con $X \dddot{\to} Y$ el conjunto de todas las funciones *parciales de* X en Y, es decir, $f : X \dddot{\to} Y \Leftrightarrow$ el dominio de f está incluido en X (pero no necesariamente coincide con todo el conjunto X) y los valores de f se toman del conjunto Y. En particular, la función $f : X_1 \times \ldots \times X_k \dddot{\to} Y$ de k argumen-

tos puede no estar definida para ciertas k-tuplas $\langle x_1, \ldots, x_k \rangle$. En particular, la función no definida en ninguna parte pertenece al conjunto $X_1 \times \ldots \times X_k \ddot{\to} Y$.

Nosotros nos ocuparemos especialmente de funciones que procesan palabras. Sea Δ un alfabeto. Con Δ^* denotaremos el conjunto de todas las palabras sobre el alfabeto Δ. Supongamos que $\Delta_1, \ldots, \Delta_k, \Delta$ son alfabetos. Las máquinas de Turing pueden ser adaptadas para el cálculo de funciones de la forma $\Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$. Para esto, tomemos una letra q que no pertenece a los alfabetos considerados, y representemos todas las k-tuplas de palabras de $\Delta_1^* \times \ldots \times \Delta_k^*$ como palabras sobre el alfabeto $\Delta_1 \cup \ldots \cup \Delta_k \cup \{q\}$. Por ejemplo, una terna ordenada $\langle x_1, x_2, x_3 \rangle$, donde $x_i \in \Delta_i^*$, es representada como la palabra $x_1 q x_2 q x_3$.

Supongamos que $f : \Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$ es una función (posiblemente, parcial) de k argumentos. Diremos que la máquina de Turing

$$M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle$$

calcula f si

1) $\Delta \cup \Delta_1 \cup \ldots \cup \Delta_k \cup \{q\} \subseteq \Sigma$;
2) para cualesquiera $x_1, \ldots, x_k$, $x_i \in \Delta_i^*$, la k-tupla $\langle x_1, \ldots, x_k \rangle$ pertenece al dominio de la función

$$f \Leftrightarrow !M(x_1 q \ldots q x_k) \quad \text{y} \quad M(x_1 q \ldots q x_k) \in \Delta^*;$$

3) para cualesquiera $x_1, \ldots, x_k$, $x_i \in \Delta_i^*$, si

$$!M(x_1 q \ldots q x_k) \quad \text{y} \quad M(x_1 q \ldots q x_k) \in \Delta^*,$$

entonces

$$f(x_1, \ldots, x_k) = M(x_1 q \ldots q x_k);$$

4) por conveniencia, exijamos también que el blanco a_0 de la máquina M se diferencie de todas las letras del alfabeto

$$\Delta_1 \cup \ldots \cup \Delta_k \cup \Delta \cup \{q\}.$$

Subrayemos que el alfabeto externo de la máquina M que calcula la función f puede ser mucha más amplio que el alfabeto $\Delta \cup \Delta_1 \cup \ldots \cup \Delta_k \cup \{q\}$. Como dicen, la máquina M está *sobre el alfabeto*

$$\Delta \cup \Delta_1 \cup \ldots \cup \Delta_k \cup \{q\}.$$

Nosotros exigimos que M se comporte «como la función f» sólo en las entradas $x_1 q \ldots q x_k$. Las letras del alfabeto externo Σ que no figuran en $\Delta \cup \ldots \cup \Delta_k \cup \{q\}$ pueden utilizarse durante el procesamiento de palabras de la forma $x_1 q \ldots q x_k$, pero sólo en las configuraciones intermedias del protocolo de cálculo. La función

$$f : \Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$$

se denomina *función computable* (según Turing) si existe una máquina de Turing que calcula f.

2.1.5 Consideremos ahora funciones definidas para números naturales,

$$f : \omega \times \ldots \times \omega \ddot{\to} \omega.$$

Para estas funciones es posible introducir de manera natural el concepto de computabilidad. Representemos los números naturales en forma de palabras sobre el alfabeto $\{|\}$:

$$0\ 1\ 2\ 3\ 4\ 5\ \ldots$$

$$\varnothing\ |\ ||\ |||\ ||||\ |||||\ \ldots$$

A veces, para diferenciar los números naturales representados de este modo de los naturales «habituales» entendidos en el sentido teórico-conjuntista (por ejemplo, según Von Neumann), las palabras de barras verticales se denominan *numerales* de los números naturales respectivos. El numeral del número n se denota mediante $\overline{n}$, por ejemplo, $\overline{3} = |||$.

Entonces toda función en números naturales, digamos,

$$f : \omega \times \omega \ddot{\to} \omega,$$

se representa naturalmente mediante cierta función

$$\overline{f} : \{|\}^* \times \{|\}^* \ddot{\to} \{|\}^*$$

definida para palabras de barras verticales:

$$f(m_1, m_2) = m_3 \Leftrightarrow \overline{f}(\overline{m}_1, \overline{m}_2) = \overline{m}_3.$$

Una función numérica se denomina *función computable* según Turing si es computable según Turing la correspondiente función en palabras de barras verticales.

Las funciones $f : \omega \times \ldots \times \omega \ddot{\to} \omega$ computables según Turing se denominan también *funciones recursivas parciales* (el término «parcial» nos recuerda que f no necesariamente está definida en todo el conjunto $\omega \times \ldots \times \omega$). Si una función recursiva parcial f de k argumentos está definida en todas las k-tuplas $\langle n_1, \ldots, n_k \rangle$ de números naturales, es decir, $f : \omega \times \ldots \times \omega \to \omega$, entonces se denomina *función recursiva total* o, simplemente, *función recursiva.*

Para resumir, una función recursiva parcial es una función para la que existe un algoritmo que la calcula expresado en forma de una máquina de Turing. En el caso de una función recursiva total, este algoritmo obligatoriamente concluye su trabajo

para cualesquiera números naturales de entrada y da el valor de la función.

Se puede demostrar que todas las funciones habituales de la teoría de números, como $x + y$, xy, x^y, $[\sqrt{x}]$, etcétera, son funciones recursivas, definidas no en todas partes, por ejemplo, x/y, $x - y[\lg(x - y)]$ son funciones recursivas parciales. La siguiente máquina M calcula la función

$$f(m, n) = m + 2n.$$

El alfabeto externo de M es $\{|, q, a_0\}$, donde a_0 es blanco. El alfabeto interno es $\{q_0, q_1, q_2, q_3, q_4, q_5\}$, donde q_0 y q_1 son los estados inicial y final, respectivamente. El programa de la máquina es el siguiente:

1. $q_0| \rightarrow q_2|$
2. $q_0q \rightarrow q_2q$
3. $q_2| \rightarrow q_2|R$
4. $q_2q \rightarrow q_2qR$
5. $q_2a_0 \rightarrow q_3a_0L$
6. $q_3 | \rightarrow q_4a_0L$
7. $q_4| \rightarrow q_4|L$
8. $q_4q \rightarrow q_4qL$
9. $q_4a_0 \rightarrow q_5 \mid L$
10. $q_5a_0 \rightarrow q_2 \mid$
11. $q_3q \rightarrow a_0q_1$

El protocolo de cálculo puede ser descrito brevemente de la siguiente manera. Supongamos que la configuración inicial es $\langle q_0 \mid\rangle \mid\mid\mid q \mid\mid$. Las instrucciones 1 y 2 trasladan la máquina al estado q_2 : $\langle q_2 \mid\rangle \mid\mid\mid q \mid\mid$. A continuación, siguiendo las instrucciones 3 y 4, se mueve hacia la derecha hasta que a la derecha aparece la celda vacía: $\mid\mid\mid\mid q \mid\mid \langle q_2, a_0\rangle$. Después, la máquina se mueve hacia la izquierda y pasa al estado q_3 :$\mid\mid\mid\mid q\langle q_3, \mid\rangle$ (instrucción 5). A continuación, la máquina borra la barra vertical leída, pasa

al estado q_4 y en este estado se mueve hacia la izquierda hasta que a la izquierda aparece la celda vacía (instrucciones 6, 7, 8): $\langle q_4, a_0\rangle$ |||| q |. Siguiendo las instrucciones 9 y 10, la máquina escribe a la izquierda dos barras verticales y se traslada nuevamente al estado q_2 : $\langle q_2$ |$\rangle$ ||||| q |. Luego, nuevamente comienzan a actuar las instrucciones 3 y 4, y el ciclo se repite, la máquina va hacia el final de la palabra, borra una barra vertical después de q, va hacia la izquierda y escribe a la izquierda dos barras verticales, y así sucesivamente, hasta que no queden barras verticales a la derecha. Después de esto aparece la configuración |||||||| $\langle q_3, q\rangle$. La instrucción 11 borra q, y la máquina se detiene en la configuración final |||||||| $\langle q_1, a_0\rangle$.

Ejercicio. Construir la máquina de Turing que calcula la función

$$f(m, n) = m \cdot n.$$

2.2 Tesis de Church

2.2.1 Parece ser evidente que toda función $f : \Sigma^* \dddot{\rightarrow} \Sigma^*$ definida en palabras y computable según Turing es efectivamente computable. En efecto, el algoritmo para el cálculo de esta función es definido propiamente por una máquina de Turing, de la que se habla en la definición de computabilidad.

En 1936 Church propuso la tesis de que *toda función efectivamente computable es computable según Turing*. Hablando más exactamente, Church no utilizó el concepto de computabilidad según Turing, sino un concepto algo diferente de computabilidad (la *definibilidad lambda de Church*), que es matemáticamente equivalente a la definición de computabilidad dada por nosotros. En virtud del análisis efectuado al inicio de la sección anterior, la tesis de Church se puede formular de otro modo: todo algoritmo de palabras, discreto, general, determinado y aislado puede ser definido en forma de una máquina de Turing.

Dicho de otro modo, las máquinas de Turing pueden imitar cualquier algoritmo del tipo indicado.

Señalemos inmediatamente que la *tesis* de Church no es una afirmación matemática, puesto que en su formulación figura el concepto de algoritmo en el sentido intuitivo del término. Por esta razón, la tesis de Church no puede ser demostrada ni refutada en el marco de la práctica matemática tradicional. No es un resultado matemático, sino más bien una observación de las ciencias naturales. No obstante, en favor de la tesis de Church se pueden dar serias razones de carácter científico-natural.

En primer lugar, durante muchos siglos de desarrollo en la matemática se ha acumulado una gran cantidad de algoritmos. Todos ellos son computables según Turing. Este material experimental debe convencernos de la veracidad de la tesis de Church no menos que, por ejemplo, los correspondientes experimentos convencen a los físicos de que la ley de conservación de la energía es cierta.

En segundo lugar, casi al mismo tiempo que el concepto de computabilidad según Turing, fueron propuestos otros modos de abordar el concepto de computabilidad, que exteriormente se diferenciaban mucho entre sí. Sin embargo, todos ellos resultaron equivalentes. Mencionemos algunos de ellos:

- el cálculo ecuacional de Herbrand—Gödel;
- las funciones recursivas parciales según Kleene;
- la definibilidad lambda de Church;
- los sistemas canónicos de Post;
- los algoritmos normales de Márkov;
- los algoritmos de Kolmogórov—Uspenski.

En tercer lugar, intuitivamente las funciones efectivamente computables deben formar un conjunto cerrado respecto a

algunas operaciones importantes, como la composición, la ramificación, la iteración, etcétera. Resulta que, como era de esperar, la familia de funciones computables según Turing es cerrada respecto a estas operaciones.

Finalmente, señalemos que la tesis de Church *no es necesaria* desde el punto de vista puramente matemático y, propiamente, nunca se utiliza en las afirmaciones matemáticas. En los razonamientos matemáticos donde es necesaria la computabilidad, siempre se puede utilizar la computabilidad según Turing.

La tesis de Church es importante para las aplicaciones de la matemática en las ciencias naturales. Ella explica el importante papel que desempeña el concepto de algoritmo en una forma exacta (por ejemplo, en forma de la computabilidad según Turing) en la matemática moderna.

Por ejemplo, a veces se logra demostrar rigurosamente que una función concreta $f : \Sigma^* \ddot{\to} \Sigma^*$ no es computable según Turing. La tesis de Church nos indica que sería inútil de hecho buscar un algoritmo (en el sentido intuitivo de esta palabra) que calcule f.

La función f tampoco será computable intuitivamente.

De esta manera, aparece una valiosa posibilidad para determinar con ayuda de medios matemáticos exactos la no computabilidad de algunas funciones.

2.3 Conjuntos y predicados recursivos y recursivamente enumerables

2.3.1 En la sección anterior se dio la definición de función computable. Ahora trataremos de definir qué se debe entender por predicado computable. Para esto debemos considerar, por supuesto, *predicados de palabras* $P(x_1, \ldots, x_k)$, donde x_i son palabras sobre cierto alfabeto, por ejemplo, x_1 denota palabras sobre el alfabeto Δ_1, x_2 denota palabras sobre el alfabeto Δ_2, y así sucesivamente. De este predicado P se dice que es de tipo $\Delta_1^* \times \ldots \times \Delta_k^*$, lo que indica la región de variación de cada argumento.

Al predicado de palabras P se le puede asignar una función $\chi_P : \Delta_1^* \times \ldots \times \Delta_k^* \to \{0, 1\}$ (denominada *función característica* del predicado) tal que para toda k-tupla $\langle x_1, \ldots, x_k \rangle$, donde $x_i \in \Delta_i*$,

$$P(x_1, \ldots, x_k) \text{ es verdadero } \Leftrightarrow \chi_P(x_1, \ldots, x_k) = 1.$$

Por otra parte, a un predicado de palabras se le puede asignar el *conjunto relación* del predicado dado, es decir, el conjun-

to $X_P \subseteq \Delta_1^* \times \ldots \times \Delta_k^*$ tal que

$$P(x_1, \ldots, x_k) \text{ es verdadero } \Leftrightarrow \langle x_1, \ldots, x_k \rangle \in X_P.$$

Y viceversa, si está dado un conjunto de palabras $X \subseteq \Sigma^*$, entonces se puede considerar el predicado de pertenencia de este conjunto: para toda palabra $x \in \Sigma^*$,

$$P(x) \text{ es verdadero} \Leftrightarrow x \text{ pertenece a } X.$$

Con mayor frecuencia se consideran predicados de palabras para los que los alfabetos $\Delta_1, \ldots, \Delta_k$ coinciden. Por ejemplo, los predicados definidos en los números naturales (*predicados aritméticos*) se pueden interpretar como predicados de palabras definidos en numerales, es decir, en palabras sobre el alfabeto $\{|\}$.

2.3.2 Primera definición de computabilidad. Un predicado P de tipo $\Delta_1^* \times \ldots \times \Delta_k^*$ se denomina *recursivo* (o bien *decidible*) si la función característica correspondiente χ_P es computable según Turing.

Intuitivamente el predicado P es recursivo si existe un algoritmo que para todo conjunto $\langle x_1, \ldots, x_k \rangle$ de palabras permite determinar si $P(x_1, \ldots, x_k)$ es o no verdadero.

Repitamos la definición de predicado recursivo en términos de una máquina de Turing. Un predicado P de tipo $\Delta_1^* \times \ldots \times \Delta_k^*$ se denomina *recursivo* (o bien *decidible*) si existe una máquina de Turing $M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle$ tal que

1) $\Delta_1 \cup \ldots \cup \Delta_k \cup \{0, 1\} \cup \{q\} \subseteq \Sigma$,
donde, como antes, q es una nueva letra que denota conjuntos de palabras;

2) para cualesquiera $x_1, \ldots, x_k$ ($x_i \in \Delta_i^*$) está definido el valor de $M(x_1 q \ldots q x_k)$, y este valor es igual, o bien a 0, o bien a 1;
3) $P(x_1, \ldots, x_k)$ es verdadero si y sólo si $M(x_1 q \ldots q x_k) = 1$.

Un conjunto $X \subseteq \Sigma^*$ se denomina *recursivo* si el correspondiente predicado de pertenencia $x \in X$, donde x varía en el conjunto Σ^*, es recursivo.

Los *predicados aritméticos* habituales $x \leqslant y$, $x + y = z$, «x es un número primo», «y es divisible por x» son recursivos. La demostración rigurosa de esta afirmación se basa en la construcción de las correspondientes máquinas de Turing. Pero incluso sin realizar esta construcción la decidibilidad de estos predicados debe ser evidente para el lector. En efecto, es evidente que existe un método efectivo para comprobar si es cierto que, por ejemplo, y es divisible por x para dos números naturales x e y. En lo sucesivo, por lo general omitiremos la construcción concreta de las máquinas de Turing en los casos cuando es claro que el algoritmo necesario existe. Los métodos de construcción de máquinas de Turing se consideran en libros de lógica matemática más detallados (véase la bibliografía).

Asimismo, son recursivos muchos de los conjuntos usuales de números naturales: el conjunto de los números pares, el conjunto de los números primos, el conjunto de los números divisibles por 7, etcétera. Un número se denomina *perfecto* si es igual a la suma de sus divisores (diferentes del número dado). El conjunto de todos los números perfectos impares es recursivo, ya que existe un método simple para aclarar si un número dado es impar y perfecto. No obstante, hasta ahora no se sabe si este conjunto es vacío o no, ya que no se sabe si existen números con estas propiedades.

2.3.3 **Segunda definición de computabilidad.** La *enumerabilidad recursiva* de un predicado impone menos exigencias sobre el correspondiente algoritmo.

Intuitivamente, un predicado P es *recursivamente enumerable* si existe un método que permite establecer la veracidad de $P(x_1, \ldots, x_k)$ en el caso cuando $P(x_1, \ldots, x_k)$ es verdadero. Si $P(x_1, \ldots, x_k)$ es falso, entonces este método a veces será capaz de demostrar esto, pero en otras ocasiones continuará indefinidamente. De esta manera, al comprobar la veracidad para una k-tupla dada $x_1, \ldots, x_k$, no se puede asegurar que obtendremos una respuesta.

La definición exacta es la siguiente. Un predicado P de tipo $\Delta_1^* \times \ldots \times \Delta_k^*$ se denomina *recursivamente enumerable* si existe una máquina de Turing $M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle$ tal que

1) $\Delta_1 \cup \ldots \cup \Delta_k \cup \{0, 1\} \cup \{q\} \subseteq \Sigma$;
2) para cualesquiera $x_1, \ldots, x_k$ $(x_i \in \Delta_i^*)$, *si está definido el valor de* $M(x_1 q \ldots q x_k)$, entonces este valor es igual, o bien a 0, o bien a 1;
3) $P(x_i, \ldots, x_k)$ es verdadero si y sólo si $M(x_1 q \ldots q x_k) = 1$.

Un conjunto $X \subseteq \Sigma^*$ se llama *recursivamente enumerable* si el correspondiente predicado de pertenencia es recursivamente enumerable.

2.3.4 De las definiciones se deduce que *todo predicado (conjunto) recursivo es también recursivamente enumerable.*

Lema. *Si el predicado* $P(x_1, \ldots, x_k, y)$ *es recursivamente enumerable, entonces es recursivamente enumerable el predicado*

$$\exists y P(x_1, \ldots, x_k, y).$$

► Supongamos que y varía en el conjunto Δ^*, y que M es la máquina que figura en la definición de enumerabilidad recursiva del predicado $P(x_1, \ldots, x_k, y)$. Comprobemos que para el predicado $\exists\, yP(x_1, \ldots, x_k, y)$ la correspondiente máquina M' existe. No escribiremos el programa M', sólo describiremos en términos informales cómo M' funciona. Esperamos que después de estas aclaraciones la construcción de M' no presente dificultades para el lector (aunque seguirá siendo una tarea voluminosa). Contemos todas las palabras sobre el alfabeto Δ en forma de una sucesión efectivamente definida:

$$Y_1, Y_2, Y_3, \ldots .$$

Consideremos la k-tupla $x_1, \ldots, x_k$ y describamos el proceso de obtención del valor de $M'(x_1 q \ldots q x_k)$.

Los cálculos se realizan por etapas. En la primera etapa, la máquina M' forma el conjunto $x_1 q \ldots q x_k Y_1$ y realiza un paso para calcular el valor de $M(x_1 q \ldots q x_k q Y_1)$. Si en un paso se detecta que $M(x_1 q \ldots q x_k q Y_1) = 1$, entonces la máquina M' finaliza su trabajo, y tomamos $M'(x_1 q \ldots q x_k) = 1$.

En la segunda etapa (si en la primera el trabajo no concluyó), la máquina M' realiza dos pasos para calcular dos valores:

$$M(x_1 q \ldots q x_k q Y_1)$$

y

$$M(x_1 q \ldots q x_k q Y_2).$$

Si en estos dos pasos de cálculo de M se detecta que al menos uno de los dos valores es igual a la unidad, entonces concluimos el trabajo de M', y tomamos $M'(x_1 q \ldots q x_k) = 1$. En la tercera etapa (si en las etapas anteriores el trabajo concluyó), la máquina

M' realiza tres pasos para calcular tres valores:

$$M(x_1 q \dots q x_k q Y_1),$$
$$M(x_1 q \dots q x_k q Y_2),$$
$$M(x_1 q \dots q x_k q Y_3).$$

Si en estos tres pasos de cálculo de M se detecta que al menos uno de estos tres valores es igual a la unidad, entonces concluimos el trabajo de M', y tomamos $M'(x_1 q \dots q x_k) = 1$. De esta manera, sucesivamente, efectuamos una etapa tras otra.

Si en una etapa se calcula el valor $M(x_1 q \dots q x_k q Y_i) = 0$, entonces excluimos el conjunto $x_1 q \dots q x_k q Y_i$ de la lista de sometidos a prueba, pero debido a este conjunto no concluimos el trabajo, y pasamos a la siguiente etapa en búsqueda de un conjunto para el que $M(x_1 q \dots q x_k q Y_i) = 1$. La máquina M' será la que confirma la enumerabilidad recursiva de $\exists\, y P(x_1, \dots, x_k, y)$.

Nótese que M' sólo toma el valor 1 o no está definida. Por tanto, incluso si $P(x_1, \dots, x_k, y)$ es un predicado recursivo, la máquina M' sólo confirma la enumerabilidad recursiva de $\exists\, y P(x_1, \dots, x_k, y)$. En efecto, como veremos más adelante, se puede construir un predicado recursivo P tal que el predicado $\exists\, y P$ es recursivamente enumerable, pero no es recursivo. ◄

Lema. *Para todo predicado recursivamente enumerable* $Q(x_1, \dots, \dots x_k)$, *existe un predicado recursivo* $P(x_1, \dots, x_k, y)$ *tal que*

$$Q(x_1, \dots, x_k) \Leftrightarrow \exists\, y P(x_1, \dots, x_k, y).$$

► Sea M la máquina que figura en la definición de enumerabilidad recursiva de Q. Consideremos el siguiente predicado: $P(x_1, \dots, x_k, y)$ es verdadero $\Leftrightarrow$ y es un protocolo finito de cálculo de la máquina M tal que en la configuración inicial y en la cinta

está escrito el conjunto $x_1 q \ldots q x_k$, y en la configuración final y en la cinta está escrita la unidad. Consideraremos los protocolos finitos de M como palabras sobre un alfabeto apropiado Δ, de modo que $y \in \Delta^*$.

Se puede demostrar que el predicado P es decidible. Es evidente intuitivamente que para una palabra dada y se puede determinar efectivamente si y es realmente un protocolo de cálculo de la máquina M y qué está escrito en la cinta para diferentes configuraciones del protocolo y. La demostración rigurosa (que omitimos) se basa en la construcción (bastante engorrosa) de la correspondiente máquina de reconocimiento.

Ahora, de acuerdo con una propiedad de la máquina M, tenemos

$$Q(x_1, \ldots, x_k) \Leftrightarrow \exists\, y P(x_1, \ldots, x_k, y). \quad \blacktriangleleft$$

Este lema justifica el término «enumerable» utilizado para un predicado recursivamente enumerable Q. Para verificar la veracidad de $Q(x_1, \ldots, x_k)$, se deben enumerar sucesivamente todas las palabras $Y_1, Y_2, \ldots$ sobre cierto alfabeto Δ y verificar sucesivamente la veracidad del predicado recursivo P:

$$P(x_1, \ldots, x_k, Y_1), \quad P(x_1, \ldots, x_k, Y_2), \quad \ldots.$$

Si Q es verdadero, entonces este proceso termina, y hallamos el correspondiente Y_i. Si Q es falso, entonces el proceso continuará indefinidamente y es muy probable que no lleguemos a saber que Q es falso.

2.3.5 Señalemos que si se aplican las conectivas lógicas $\wedge$, $\vee$, $\supset$ y $\neg$ a los predicados recursivos, obtendremos predicados recursivos.

La demostración consiste en la construcción de las máquinas de reconocimiento para los predicados compuestos a partir de las máquinas de los predicados componentes. Intuitivamente, el método de reconocimiento de la veracidad (por ejemplo, del predicado $P(x_1, \ldots, x_k) \vee Q(x_1, \ldots, x_k)$) es evidente si es conocido el método de reconocimiento de la veracidad para P y Q.

En lo que respecta a los predicados recursivamente enumerables, la aplicación de las conectivas lógicas $\wedge$, $\vee$ a ellos origina nuevamente predicados recursivamente enumerables. Sin embargo, esto no es válido para las conectivas $\supset$ y $\neg$ en el caso general. Más adelante veremos un ejemplo de un predicado recursivamente enumerable cuya negación no es recursivamente enumerable.

Si consideramos las relaciones que corresponden a los predicados, entonces de las observaciones anteriores se deduce que la unión y la intersección de cualesquiera dos conjuntos recursivos (recursivamente enumerables) es nuevamente un conjunto recursivo (recursivamente enumerable). El complemento de un *conjunto recursivo de palabras* sobre cierto alfabeto (respecto al conjunto de todas las palabras sobre este alfabeto) es también un conjunto recursivo. Sin embargo, el complemento de un conjunto recursivamente enumerable puede no ser recursivamente enumerable.

En el lenguaje de la aritmética Ar es natural dar las siguientes definiciones:

$$x \leqslant y \leftrightharpoons \exists z(x + z = y),$$

$$x < y \leftrightharpoons x \leqslant y \wedge \neg(x = y).$$

Si está dado el predicado aritmético $P(x, y_1, \ldots, y_n)$, entonces se pueden definir nuevos predicados mediante la aplicación

de los *cuantificadores limitados*:

$$(\forall\, x \leqslant z)P(x, y_1, \ldots, y_n) \leftrightharpoons \forall\, x(x \leqslant z \supset P(x, y_1, \ldots, y_n));$$

$$(\exists\, x \leqslant z)P(x, y_1, \ldots, y_n) \leftrightharpoons \exists\, x(x \leqslant z \wedge P(x, y_1, \ldots, y_n));$$

$$(\forall\, x < z)P(x, y_1, \ldots, y_n) \leftrightharpoons \forall\, x(x < z \supset P(x, y_1, \ldots, y_n));$$

$$(\exists\, x < z)P(x, y_1, \ldots, y_n) \leftrightharpoons \exists\, x(x < z \wedge P(x, y_1, \ldots, y_n)).$$

Los predicados obtenidos son predicados de los argumentos $z, y_1, \ldots, y_n$. Nótese que

$$\neg(\forall\, x \leqslant z)P(x, y_1, \ldots, y_n) \Leftrightarrow (\exists\, x \leqslant z)\neg P(x, y_1, \ldots, y_n).$$

Ejercicio. Indicar leyes análogas para la transformación de la negación de los demás cuantificadores limitados.

La aplicación de un cuantificador limitado a un predicado recursivo (recursivamente enumerable) origina un predicado recursivo (recursivamente enumerable). La demostración de esta afirmación se basa en la construcción, a partir de las máquinas de Turing de los predicados iniciales, de las correspondientes máquinas de Turing para los predicados resultantes.

2.3.6 Teorema de Post. *Si ambos predicados P y $\neg P$ son recursivamente enumerables, entonces ellos son recursivos.*

► Supongamos que P y $\neg P$ son predicados de tipo $\Delta_1^* \times \times \ldots \times \Delta_k^*$, y que M_1 y M_2 son las máquinas de Turing que figuran en la definición de enumerabilidad recursiva de P y $\neg P$, respectivamente. Definamos la máquina M' que reconoce la veracidad del predicado P, por ejemplo. Como en las anteriores ocasiones, no escribiremos el programa de M', sino sola-

mente describiremos cómo M' funciona. Consideremos la k-tupla $\langle x_1, \ldots, x_k \rangle$ y describamos el proceso de obtención del valor de $M'(x_1 q \ldots q x_k)$. Los cálculos se realizan por etapas. En la primera etapa, la máquina M' realiza un paso del cálculo de los valores de $M_1(x_1 q \ldots q x_k)$ y $M_2(x_1 q \ldots q x_k)$. En la segunda etapa, se realizan dos pasos del cálculo de los valores de $M_1(x_1 q \ldots q x_k)$ y $M_2(x_1 q \ldots q x_k)$. En la tercera, tres pasos del cálculo de estos dos valores, y así sucesivamente. El cálculo finaliza en cuanto se calcula uno de los valores, el de $M_1(x_1 q \ldots q x_k)$ o el de $M_2(x_1 q \ldots q x_k)$. Si se detecta que, o bien $M_1 = 1$, o bien $M_2 = 0$, entonces tomamos $M' = 1$. Si resulta que, o bien $M_1 = 0$, o bien $M_2 = 1$, entonces tomamos $M' = 0$.

De la definición de las máquinas M_1 y M_2, se deduce que son imposibles el caso $M_1 = 1$ y $M_2 = 1$ (esto significaría que para $\langle x_1, \ldots, x_k \rangle$ son verdaderos simultáneamente P y $\neg P$) y el caso $M_1 = 0$ y $M_2 = 0$ (lo que significaría que $\langle x_1, \ldots, x_k \rangle$ no es satisfecha ni por P, ni por $\neg P$). Por otro lado, necesariamente, o bien $M_1(x_1 q \ldots q x_k) = 1$, o bien $M_2(x_1 q \ldots q x_k) = 1$, puesto que $P(x_1, \ldots, x_k)$ o $\neg P(x_1, \ldots, x_k)$. De aquí se deduce que el algoritmo M' reconoce la veracidad del predicado P. ◀

2.3.7 Recordemos algunos resultados de la teoría de algoritmos relacionados directamente con la lógica.

Es obvio que las fórmulas y los términos de un lenguaje lógico-matemático como ZF^+ pueden ser interpretados como palabras sobre un alfabeto Σ apropiado. En efecto, como se deduce de la definición de la subsección 1.2.1, las expresiones de ZF^+ se construyen con ayuda de los símbolos , (coma formal), $(,), \in, \wedge, \vee, \supset, \neg, \forall, \exists, \{, \}, |, \varnothing, \omega, P, \cup, \mapsto$ y de un conjunto

infinito de variables. Pero las variables pueden, a su vez, ser consideradas como palabras formadas por los símbolos v y $|$, y paréntesis: $x \leftrightharpoons (v\,|)$, $y \leftrightharpoons (v\,||)$, $z \leftrightharpoons (v\,|||)$, etcétera.

Análogamente, las expresiones de los lenguajes Ar, Ar2 y ZF también pueden ser interpretadas como palabras sobre alfabetos apropiados. Esto sucede porque las expresiones de los lenguajes considerados se construyen a partir de un número finito de símbolos indicados explícitamente y según reglas estrictamente definidas. Denominemos estos lenguajes *explícitamente definidos*. Aquí no daremos la definición matemática precisa de lenguaje explícitamente definido. Si el lector desea, como lenguaje de este tipo puede entender uno de los lenguajes lógico-matemáticos concretos descritos en el presente libro, aunque los resultados generales que veremos también son válidos para muchos otros lenguajes. Sin embargo, se debe tener en cuenta que, en principio, se pueden considerar también lenguajes lógico-matemáticos cuyas expresiones se definen mediante métodos indirectos teórico-conjuntistas. Para estos lenguajes, puede ser imposible representar sus expresiones en forma de palabras sobre cierto alfabeto. Éste es el caso de, por ejemplo, los lenguajes que contienen un conjunto no numerable de constantes. No obstante, los lenguajes utilizados en la construcción de las teorías axiomáticas formales, por lo general, son explícitamente definidos.

De esta manera, un lenguaje explícitamente definido Ω define un alfabeto Σ_Ω tal que las expresiones de Ω son palabras especiales sobre este alfabeto. Suponemos que el conjunto Fm_Ω de todas las fórmulas del lenguaje Ω y el conjunto Tm_Ω de todos los términos del lenguaje Ω son subconjuntos recursivos del conjunto Σ_Ω^* de todas las palabras sobre el alfabeto Σ_Ω.

Con relación a un lenguaje concreto, por ejemplo, ZF^+, esto puede ser demostrado rigurosamente mediante la construcción de la correspondiente máquina de Turing. El correspondiente procedimiento de reconocimiento debe ser claro intuitivamente, incluso sin esta voluminosa construcción: para cada palabra sobre el alfabeto del lenguaje siempre se puede determinar si ella es una fórmula de ZF^+ o no.

Luego, el conjunto A_{X_Ω} de todos los axiomas del cálculo de predicados del lenguaje explícitamente definido Ω es también un subconjunto recursivo de Σ_Ω^*, ya que para cada fórmula se puede determinar si ella tiene forma de un axioma del cálculo de predicados o no (por ejemplo, si la fórmula considerada tiene la forma $A \supset (B \supset A)$ o no).

Un árbol de fórmulas en el lenguaje Ω se definió (véase la introducción del presente libro) como cierta figura bidimensional, pero debe quedar claro que un árbol de fórmulas de un lenguaje explícitamente definido puede ser interpretado también como una palabra sobre cierto alfabeto. Por ejemplo, en lugar de $\dfrac{D_1, D_2}{A}$ se puede escribir $(D_1, D_2/A)$, etcétera. En este caso, es esencial que el conjunto de todos los árboles de deducción es un subconjunto recursivo del conjunto de todas las palabras sobre este alfabeto, ya que para una palabra se puede determinar efectivamente si ella es un árbol de fórmulas y si se cumple en dicho árbol la exigencia estructural necesaria.

Señalemos ahora que el conjunto de los axiomas no lógicos en las teorías axiomáticas formales que hemos considerado, como Ar, Ar2 y ZF, es también un conjunto recursivo, y éstas son teorías en lenguajes explícitamente definidos. Denomina-

remos a estas teorías axiomáticas *teorías explícitamente definidas*. Aquí no daremos la definición matemática exacta de teoría explícitamente definida, el lector puede considerar que se trata sencillamente de una de las teorías consideradas por nosotros.

Tomemos un alfabeto Σ_0 suficientemente extenso para que las deducciones de todas las teorías axiomáticas formales explícitamente definidas (todas las que nos interesan) se escriban como palabras sobre el alfabeto Σ_0.

Sea T una teoría axiomática formal explícitamente definida. Consideremos un predicado $\mathrm{Prf}_T(y, x)$, donde x e y son palabras sobre el alfabeto Σ_0. A saber, $\mathrm{Prf}_T(y, x)$ es verdadero si y sólo si y es un árbol de deducción de la teoría T con fórmula inferior x. Un resultado importante es que este predicado es recursivo. Para una teoría concreta, por ejemplo, para ZF, esto puede ser verificado cuidadosamente mediante la construcción de la correspondiente máquina de Turing, pero, incluso sin realizar dicha construcción, el procedimiento de reconocimiento de la veracidad de este predicado es obvio: para una palabra dada y se debe primeramente establecer si ella es una deducción en la teoría T y, seguidamente, es necesario determinar si es cierto que la fórmula inferior de esta deducción es la fórmula x.

Para la teoría explícitamente definida T, consideremos el predicado $\mathrm{Pr}_T(x)$, donde x es una palabra sobre el alfabeto Σ_0. A saber, $\mathrm{Pr}_T(x)$ es verdadero si y sólo si x es una fórmula deducible en la teoría T. Evidentemente, $\mathrm{Pr}_T(x) \Leftrightarrow \exists\, y \mathrm{Prf}_T(y, x)$.

De aquí se deduce el siguiente teorema.

Teorema. *El conjunto de las fórmulas deducibles en una teoría axiomática formal T explícitamente definida es recursivamente enumerable. En particular, el conjunto de fórmulas deducibles en*

el cálculo de predicados de un lenguaje explícitamente definido es recursivamente enumerable.

► Véase la subsección 2.3.4. ◄

Denotemos con $[T]$ el conjunto de todas las sentencias deducibles en la teoría T. Para las teorías explícitamente definidas este conjunto es recursivamente enumerable. Una teoría se denomina *decidible* si este conjunto es recursivo. Se sabe que las teorías Ar, Ar2 y ZF no son decidibles. Es interesante que algunas teorías axiomáticas formales importantes son decidibles. Éste es el caso, por ejemplo, de la teoría elemental de los números reales (véase [17]).

Denotemos con $\mathrm{Th}_{\mathrm{Ar}}(\omega)$ el conjunto de todas las sentencias del lenguaje Ar que son verdaderas en el modelo estándar ω. Se sabe que este conjunto no es ni siquiera recursivamente enumerable.

En virtud del conocido teorema de completitud de Gödel, el conjunto de todas las leyes lógicas del lenguaje Ω coincide con el conjunto de las fórmulas deducibles en el cálculo de predicados de este lenguaje. De esta manera, para un lenguaje explícitamente definido el conjunto de todas sus leyes lógicas resulta recursivamente enumerable. Para los lenguajes que hemos considerado hasta ahora, el conjunto de las leyes lógicas no es recursivo. Pero se pueden indicar lenguajes simples para los que este conjunto es recursivo. Así es el caso, por ejemplo, de un lenguaje con un tipo de variables, sin constantes y símbolos de función y con un conjunto finito de *predicados monádicos* (ésta es la denominada *teoría de predicados monádicos*).

2.4 Funciones recursivas primitivas. Numeración de Gödel. Aritmética con términos recursivos primitivos

2.4.1 Definamos a continuación una importante clase de funciones aritméticas recursivas generales. Las funciones de esta clase se denominan *funciones recursivas primitivas.*

Para esto, definamos inductivamente el concepto de *descripción recursiva primitiva* (RP). Toda descripción RP es una palabra de la forma $(k, l, \ldots)$, donde k, l son números naturales. El número l, $l > 0$, se denomina *número de argumentos de la descripción.* A toda descripción RP se le asigna una función aritmética: una función recursiva primitiva *que tiene la descripción dada.* Esta definición contiene siete puntos. Los primeros tres constituyen la base de la inducción; los últimos son la hipótesis de inducción, y muestran cómo se pueden construir nuevas descripciones RP a partir de las que ya se tienen.

1) $(1, 1), F(x) = x + 1.$
2) $(2, 1), F(x) = x.$

3) $(3, 1, m)$, $F(x) = m$ para todo número natural m.

4) Si $l > 0$, $1 \leqslant i_1, \ldots, i_s \leqslant l$ y g es una descripción RP de s argumentos a la que se le ha asignado la función G, entonces se puede definir la descripción RP $(4, l, g, i_1, \ldots, i_s)$, a la que se le asigna la función

$$F(x_1, \ldots, x_l) = G(x_{i_1}, \ldots, x_{i_s}).$$

En este caso, se dice que F se obtiene de G por intercambio, identificación e introducción de argumentos ficticios.

5) Si g es una descripción RP de l argumentos a la que se le ha asignado la función G y h es una descripción RP de p argumentos a la que se le ha asignado la función H, entonces se puede definir la descripción RP $(5, l+p-1, g, h)$, a la que se le asigna la función

$$F(y_1, \ldots, y_p, x_2, \ldots, x_l) = G(H(y_1, \ldots, y_p), x_2, \ldots, x_l).$$

En este caso, se dice que F se obtiene de G y H por reemplazo.

6) Si g es una descripción RP de dos argumentos a la que se le ha asignado una función G y m es un número natural arbitrario, entonces se puede formar la descripción RP $(6, 1, g, m)$, a la que se le asigna la función F que satisface las siguientes identidades:

$$\begin{cases} F(0) = m, \\ F(x+1) = G(x, F(x)). \end{cases}$$

En este caso, se dice que F se obtiene de G y m mediante recursión primitiva.

7) Si h es una descripción RP de m argumentos y g es una descripción RP de $m+2$ argumentos, entonces se puede definir la descripción RP $(7, m+1, g, h)$, a la cual se le asigna la función

$$\begin{cases} F(0, x_1, \ldots, x_m) = H(x_1, \ldots, x_m), \\ F(x+1, x_1, \ldots, x_m) = G(x, F(x, x_1, \ldots, x_m), x_1, \ldots, x_m). \end{cases}$$

En este caso, también decimos que F se obtiene de las funciones G y H por recursión primitiva.

Una función aritmética se denomina *recursiva primitiva* si ella ha sido asignada de acuerdo con las reglas indicadas anteriormente a cierta descripción RP.

Ejercicio. Denotemos con $+$ una función recursiva primitiva de dos argumentos que tiene la siguiente descripción RP:

$$(7, 2(4, 3(1, 1), 2), (2, 1)).$$

Comprobar que se cumplen las siguientes identidades:

$$y + 0 = y;$$
$$y + (x+1) = (y+1) + 1.$$

Construir una descripción RP natural para la función de multiplicación de dos números naturales.

Es evidente que toda función RP es computable, puesto que el método de definición de esta función con ayuda de una descripción recursiva primitiva ofrece al mismo tiempo un método de cálculo de los valores de la función para cualesquiera valores numéricos de sus argumentos. La afirmación matemática exacta se puede enunciar de la siguiente manera: *toda función recursiva*

primitiva es una función recursiva total. Para demostrar esta afirmación se debe indicar la correspondiente máquina de Turing para cada descripción recursiva primitiva. Esta construcción se lleva a cabo por inducción respecto a la longitud de la descripción RP considerada.

La afirmación recíproca, como veremos más adelante, no es válida: existen funciones recursivas totales que no son recursivas primitivas. No obstante, las funciones RP forman una amplia clase de funciones computables que es cerrada respecto a muchas de las operaciones naturales: todas las funciones recursivas totales definidas en la práctica son por lo general recursivas primitivas.

Un predicado aritmético $P(x_1, \ldots, x_n)$ se denomina *recursivo primitivo* si existe una función recursiva primitiva $f(x_1, \ldots, x_n)$ que toma como valores sólo 0 y 1 y tal que

$$P(x_1, \ldots, x_n) \Leftrightarrow f(x_1, \ldots, x_n) = 1.$$

A menudo omitiremos la comprobación de que unas u otras funciones o predicados son recursivos primitivos cuando esto va acompañado de cálculos voluminosos. Métodos detallados para realizar esta comprobación han sido son desarrollados, por ejemplo, en [9, 14, 16].

2.4.2 Con ayuda de funciones recursivas primitivas se puede definir la correspondencia biunívoca entre los pares de números naturales y los números naturales.

A saber, se pueden definir tres funciones RP $j(x, y)$, $j_1(z)$ y $j_2(z)$ tales que se cumplen las siguientes identidades:

$$j_1(j(x,y)) = x,$$
$$j_2(j(x,y)) = y,$$
$$j(j_1(z), j_2(z)) = z.$$

Por ejemplo, podemos definir la primera función de la siguiente manera:

$$j(x,y) = (\max^2\{x,y\} + y) + (\max\{x,y\} - x).$$

En este caso, además se cumple que

$$j(0,0) = 0, \quad x \leqslant j(x,y), \quad y \leqslant j(x,y).$$

Luego, la numeración de las n-tuplas de números naturales para todo n puede ser definida, por ejemplo, con ayuda de las siguientes funciones recursivas primitivas:

$$\nu_1(x) = x,$$
$$\nu_2(x_1,x_2) = j(x_1,x_2),$$
$$\nu_{n+1}(x_1,x_2,\ldots,x_{n+1}) = j(x_i,\nu_n(x_2,\ldots,x_n)),$$

para las que existen las respectivas funciones RP inversas:

$$\delta_i^n(\nu_n(x_1,\ldots,x_n)) = x_i,$$

donde $n \geqslant 1$, $1 \leqslant i \leqslant n$.

Finalmente, para cualquier n, es posible introducir una correspondencia recursiva primitiva biunívoca única entre las n-tuplas de números naturales y los números naturales. Más exactamente, para todo número natural $n \geqslant 1$ definimos la función

$$c(x_0,\ldots,x_{n-1}) = j(n-1,\nu_n(x_0,\ldots,x_{n-1})) + 1,$$

y al conjunto vacío de números naturales (para $n = 0$) se le asigna el número 0.

De esta manera, en dependencia del método de codificación, los números naturales pueden ser identificados con pares, ternas y, en general, con cualesquiera tuplas de números naturales.

Mencionemos algunas funciones recursivas primitivas más relacionadas con la numeración introducida. La función RP diádica $x * y$ de concatenación de tuplas es tal que

$$c(x_0, \ldots, x_{m-1}) * c(y_0, \ldots, y_{n-1}) = c(x_0, \ldots, x_{m-1}, y_0, \ldots, y_{n-1}),$$

$$x * 0 = 0 * x = x.$$

La función RP diádica $[x]_z$ «extrae» un elemento de la tupla x: $[0]_z = 0$, $[c(x_0, x_1, \ldots, x_{n-1})]_z = x_z$ para $z < n$ y $[c(x_0, x_1, \ldots, x_{n-1})]_z = 0$ para $z \geqslant n$. La función recursiva primitiva $\mathrm{lh}\,(x)$ determina la longitud de la tupla:

$$\mathrm{lh}\,(0) = 0, \quad \mathrm{lh}\,(c(x_0, x_1, \ldots, x_{n-1})) = n.$$

2.4.3 Nuestro objetivo es utilizar los números naturales para numerar sistemáticamente las palabras sobre diferentes alfabetos. Ante todo nos interesan las palabras sobre el alfabeto Σ_0 (véase la subsección 2.3.7), que denominaremos *alfabeto fundamental*. Supondremos que el alfabeto fundamental contiene las letras q y $|$, de modo que en él se pueden escribir naturalmente conjuntos de números naturales si se identifican los números naturales con palabras sobre el alfabeto $|$.

Fijemos una sucesión infinita de diferentes símbolos-letras: $a_0, a_1, a_2, \ldots$, que denominaremos *sucesión fundamental de letras*. Un alfabeto se denomina *simple* si consta de un número finito de letras de la sucesión fundamental. Un alfabeto simple se

llamará *reducido* si él contiene sólo letras que en la sucesión fundamental figuran con índices impares. Supongamos que el alfabeto Σ_0 contiene exactamente k letras y que estas letras figuran en la sucesión fundamental como las primeras k letras con índices impares, es decir, el alfabeto Σ_0 consta exactamente de las letras $a_1, a_3, \ldots, a_{2k+1}$. Esto significa que el alfabeto fundamental es reducido.

Supongamos que A es una palabra sobre un alfabeto simple y tiene la forma $a_{i_1} a_{i_2} \ldots a_{i_m}$. Asignemos a esta palabra el número natural $\gamma A = c(i_1, \ldots, i_m)$. Para la palabra vacía consideraremos que $\gamma\Lambda = 0$. El número natural γA se denomina *número de Gödel* de la palabra A. La aplicación γ define una correspondencia biunívoca entre todas las palabras sobre los alfabetos simples y los números naturales.

Seguidamente numeremos las máquinas de Turing con ayuda de números naturales. En primer lugar nos interesan las máquinas que procesan las palabras sobre el alfabeto fundamental, es decir, las que calculan funciones del tipo $\Sigma_0^* \ddot{\to} \Sigma_0^*$. Aquí surge una dificultad debido a que estas máquinas también pueden contener otras letras utilizadas, por ejemplo, en cálculos intermedios. Una máquina de Turing se denomina *máquina de Turing reducida* si su alfabeto externo y el alfabeto de sus estados internos son alfabetos reducidos.

Lema. *Para cada máquina de Turing M que calcula una función $f : \Sigma_0^* \ddot{\to} \Sigma_0^*$ puede ser construida una máquina de Turing reducida M' que calcula la misma función.*

▶ Es suficiente sustituir biunívocamente todas las letras de los alfabetos interno y externo de la máquina M que son di-

ferentes de las letras del alfabeto fundamental por letras de la sucesión fundamental con índices impares. ◀

En particular, si $\Delta_1, \Delta_2, \ldots, \Delta_k, \Delta$ son alfabetos incluidos en el alfabeto fundamental Σ_0 que no contienen la letra q, y la máquina M calcula la función $f : \Delta_1^* \times \ldots \times \Delta_k^* \to \Delta^*$, entonces puede ser construida la máquina reducida M' que calcula la misma función.

Sea ahora M una máquina de Turing reducida,

$$M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle.$$

Entonces, M se puede interpretar como una palabra sobre un alfabeto simple. Más exactamente, supondremos que las letras $\to, R, L$ que figuran en la escritura de las instrucciones de la máquina se encuentran en la sucesión fundamental como letras con índices *pares*. Por ejemplo, éstas pueden ser las letras a_0, a_2, a_4, respectivamente. La máquina M como palabra sobre un alfabeto simple se obtiene si se escriben sucesivamente una tras otra las siguientes palabras:

1) la sucesión de las letras de Σ (para ser más específicos, podemos suponer que las letras se escriben en el orden de crecimiento de sus índices en la sucesión fundamental);
2) la letra divisoria con índice par (por ejemplo, ésta puede ser la letra a_6);
3) la sucesión de letras S;
4) la letra divisoria a_6;
5) la sucesión de instrucciones Π, $k_1 k_2 \ldots k_m$;
6) la letra divisoria a_6;
7) la palabra $q_0 q_1 a_0$.

De esta manera, cada máquina de Turing reducida se puede considerar como una palabra sobre un alfabeto simple y, por consiguiente, cada máquina de este tipo tiene un determinado número de Gödel.

Los protocolos finitos de trabajo de las máquinas de Turing también se pueden interpretar de manera evidente como palabras sobre un alfabeto simple y, por consiguiente, asignar a estos protocolos números de Gödel.

2.4.4 Sean $\Delta_1, \ldots, \Delta_k, \Delta$ alfabetos incluidos en el alfabeto fundamental que no contienen la letra divisoria q. Supongamos que f es una función del tipo $\Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$. Definamos la función

$$f^\gamma : \omega \times \ldots \times \omega \ddot{\to} \omega,$$

que «modela» el trabajo de la función en los números de Gödel. Más exactamente,

1) si en un conjunto $m_1, \ldots, m_k$ de números naturales al menos uno de los números m_i no es número de Gödel de ninguna palabra sobre el alfabeto Δ_i, entonces

$$f(m_1, \ldots, m_k) = 0;$$

2) para todo conjunto de palabras $A_1, \ldots, A_k, A$, donde

$$A_i \in \Delta_i^*, \quad A \in \Delta,$$

tenemos

$$f(A_1, \ldots, A_k) = A \Leftrightarrow f^\gamma(\gamma A_1, \ldots, \gamma A_k) = \gamma A.$$

Análogamente, para todo predicado de palabras P del tipo $\Delta_1^* \times \ldots \times \Delta_k^*$ se puede introducir un predicado aritmético modelador P^γ tal que

1) si el conjunto $m_1, \ldots, m_k$ es tal que al menos uno de los números naturales m_i no es número de Gödel de ninguna palabra del alfabeto Δ_i, entonces $P(m_1, \ldots, m_k)$ es falso;
2) para todo conjunto de palabras $A_1, \ldots, A_k, A_i \in \Delta_i^*$, tenemos $P(A_1, \ldots, A_k) \Leftrightarrow P^\gamma(\gamma A_1, \ldots, \gamma A_k)$.

Lema. *Una función f es computable si y sólo si la función f^γ es computable.*
Un predicado P es recursivo (recursivamente enumerable) si y sólo si el predicado P^γ es recursivo (recursivamente enumerable).

Omitimos la voluminosa demostración, la cual consiste en la construcción de las correspondientes máquinas a partir de las máquinas iniciales.

2.4.5 Identifiquemos los números naturales con palabras sobre el alfabeto |. El número de Gödel de un número natural como palabra no coincide con el propio número natural (a excepción del cero). Pero la correspondencia entre un número natural y su número de Gödel es recursiva primitiva. Más exactamente, se pueden construir dos funciones recursivas primitivas monádicas Gd y Gd^{-1} tales que, para todo número natural m,

$$\mathrm{Gd}(m) = \gamma m, \quad \mathrm{Gd}^{-1}(\gamma m) = m.$$

2.4.6 La numeración de Gödel ofrece la posibilidad de hablar de objetos constructivos complejos en el lenguaje de la aritmética. Nuestra intención es escribir diferentes propiedades de estos objetos en el lenguaje Ar y, a continuación, demostrarlas en la teoría axiomática formal Ar. La dificultad principal en la realización de este programa radica en que en la teoría Ar hay pocas

funciones: sólo la adición y la multiplicación. Por esta razón, formularemos la teoría axiomática Ar^+, que es más expresiva y en la cual, hablando en términos generales, para cada función recursiva primitiva existe un símbolo de función.

El lenguaje Ar^+ contiene un tipo de variables, $x, y, z, \ldots$, la constante 0, y para cada descripción recursiva primitiva p de l argumentos contiene un símbolo de función de l argumentos. Para ser más específicos, podemos considerar que la descripción RP p como palabra sobre el alfabeto (,), ,, | es precisamente este símbolo de función de Ar^+. En particular, en Ar^+ existen todos los símbolos de función de Ar (véase la introducción del presente libro). Por ejemplo, para S se tiene la descripción RP (1, 1); para $+$, la descripción RP (7, 2, (4, 3, (1, 1), 2), (2, 1)).

Los términos del lenguaje Ar^+ se construyen sucesivamente a partir de variables y de la constante 0 con ayuda de símbolos de función. Más exactamente, la definición inductiva de término del lenguaje Ar^+ está dada por los tres puntos siguientes:

1) Toda variable es un término.
2) La constante 0 es un término.
3) Si f es un símbolo de función de l argumentos, y los términos $t_1, \ldots, t_l$ ya han sido construidos, entonces se puede construir el nuevo término $f(t_1, \ldots, t_l)$.

Las fórmulas atómicas de Ar^+ tienen la forma $(t = r)$, donde t y r son términos arbitrarios del lenguaje Ar^+.

De esta manera, es natural considerar el lenguaje Ar como parte del lenguaje Ar^+: toda expresión de Ar es también una expresión del lenguaje Ar^+.

Los axiomas no lógicos de Ar^+, al igual que los axiomas no lógicos de Ar, se dividen en tres grupos: axiomas de igualdad,

axiomas de Peano y axiomas que definen las descripciones RP. Los axiomas de igualdad y los de Peano tienen la misma forma que en Ar, con la única diferencia de que en el esquema de axiomas de inducción se admite ahora cualquier fórmula del lenguaje Ar^+. Los axiomas que definen las descripciones RP simplemente repiten las identidades que, por definición, deben ser satisfechas por las funciones RP que tienen estas descripciones.

Sea m un número natural. Denotemos con $\widetilde{m}$ o $m\widetilde{\ }$ el término de Ar que tiene la forma $SS\ldots S0$, donde el símbolo de función S se toma m veces. Ésta es la representación natural del número m en el lenguaje Ar. Las siguientes igualdades formales son ejemplos de axiomas de la teoría Ar^+:

$$\begin{aligned}(2,1)(x) &= x;\\ (3,1,m)(x) &= \widetilde{m};\\ (6,1,g,m)(0) &= \widetilde{m};\\ (6,1,g,m)(Sx) &= g(x,(6,1,g,m)(x)),\end{aligned}$$

donde g es una descripción RP arbitraria de dos argumentos.

Así pues, la teoría Ar constituye una parte de la teoría Ar^+: todo lo que se deduce en Ar se deduce también en Ar^+.

La teoría Ar^+ es mucho más expresiva y permite escribir y demostrar prácticamente todas las afirmaciones habituales relacionadas con la teoría de números. En particular, si se tiene cierta experiencia en la construcción de deducciones formales, no es difícil demostrar la deducibilidad en Ar^+ de todas las propiedades necesarias de los números de Gödel de palabras sobre alfabetos simples.

2.4.7 Es interesante que, como demostró Gödel, las teorías Ar y Ar^+ resultan, en esencia, equivalentes. La explicación consiste en que, utilizando ciertos razonamientos teórico-numéricos, se logra representar las igualdades de términos complejos del lenguaje Ar^+ mediante fórmulas de la teoría Ar, es decir, mediante fórmulas que contienen sólo la adición y la multiplicación.

Más exactamente, para toda fórmula A del lenguaje Ar^+ se define su fórmula-traducción A^0 en el lenguaje Ar, la cual contiene los mismos parámetros que la fórmula A. Para cada término t del lenguaje Ar^+ y una variable y se define la fórmula $(y = t)^*$ del lenguaje Ar, la cual contiene los mismos parámetros que la fórmula $y = t$. Esta traducción posee muchas propiedades, lo que era de esperar de ella. Estas propiedades quedan expresadas por los siguientes seis lemas.

Lema 1. *Si A es una fórmula de* Ar *y t es un término de* Ar, *entonces en* Ar *son deducibles las equivalencias*

$$A^0 \equiv A,$$
$$(y = t)^* \equiv (y = t).$$

Lema 2. *Si A es una fórmula de Ar^+ y t es un término de Ar^+, entonces en Ar^+ son deducibles las equivalencias*

$$(y = t)^* \equiv (y = t).$$

Lema 3. *Si A es una fórmula de Ar^+ y t es un término de Ar^+, entonces tienen lugar las siguientes equivalencias:*

$$\mathrm{Ar}^+ \vdash A \Leftrightarrow \mathrm{Ar} \vdash A^0,$$
$$\mathrm{Ar}^+ \vdash (y = t) \Leftrightarrow \mathrm{Ar} \vdash (y = t)^*.$$

Lema 4. *Si A es una fórmula de* Ar, *entonces*

$$\mathrm{Ar}^{+} \vdash A \Leftrightarrow \mathrm{Ar} \vdash A.$$

El lema 4 demuestra que respecto al lenguaje más limitado Ar ambas teorías son equivalentes. Se puede señalar además que la traducción indicada conserva la estructura lógica de las fórmulas. Esta circunstancia da lugar a los dos lemas siguientes.

Lema 5. *En la teoría* Ar *son deducibles las siguientes equivalencias:*

$$(A \wedge B)^0 \equiv A^0 \wedge B^0,$$
$$(A \vee B)^0 \equiv A^0 \vee B^0,$$
$$(A \supset B)^0 \equiv A^0 \supset B^0,$$
$$(\neg A)^0 \equiv \neg A^0,$$
$$(\forall x A)^0 \equiv \forall x A^0,$$
$$(\exists x A)^0 \equiv \exists x A^0.$$

Aquí, A y B son fórmulas arbitrarias del lenguaje Ar^{+}.

Lema 6. *En la teoría* Ar *son deducibles las siguientes equivalencias:*

$$(t = r)^0 \equiv \exists y((y = t)^* \wedge (y = r)^*),$$
$$(A(x \parallel t))^0 \equiv \exists y((A(x \parallel y))^0 \wedge (y = t)^*),$$
$$(z = r(x \parallel t))^* \equiv \exists y((z = r(x \parallel y))^* \wedge (y = t)^*).$$

Aquí, A es una fórmula de Ar^{+}; *t, r son términos de* Ar^{+}; *la variable y no aparece libre en A, r y t.*

No nos detendremos en la formulación exacta de la traducción y en la demostración de los lemas 1–6. El lector interesado puede encontrar las técnicas necesarias para esto en [9, 14].

Señalemos para concluir que, al igual que la teoría Ar, la teoría Ar^+ es explícitamente definida. Las fórmulas, términos y deducciones de la teoría Ar^+ se interpretan naturalmente como palabras sobre el alfabeto fundamental y, por consiguiente, tienen números de Gödel.

2.5 Algunos teoremas de la teoría general de algoritmos

2.5.1 Función universal. Para todo $n \geqslant 1$ consideremos el predicado $(n+2)$-ádico de Kleene, definido en los números naturales:

$$T_n(e, x_1, \ldots, x_n, z).$$

Por definición, $T_n(e, x_1, \ldots, x_n, z)$ es verdadero si y sólo si e es el número de Gödel de una máquina (reducida) de Turing M y z es el número de Gödel del protocolo finito de cálculo Z de la máquina M, en cuya entrada se ha introducido el conjunto de números $x_1, \ldots, x_n$ (es decir, la palabra $x_1 q \ldots q x_n$, en la cual los números naturales son considerados como palabras sobre el alfabeto |), y además Z contiene una configuración final.

Es evidente que T_n es un predicado decidible, ya que para los $e, x_1, \ldots, x_n, z$ dados es posible determinar si T_n es válido o no. Un resultado importante (que no demostraremos aquí; el lector puede hallar los detalles en [10], por ejemplo) es que este predicado es *recursivo primitivo*, es decir, existe una función recur-

siva primitiva $t_n(e, x_1, \ldots, x_n, z)$ que toma sólo los valores 0 y 1 y

$$T_n(e, x_1, \ldots, x_n, z) \Leftrightarrow t_n(e, x_1, \ldots, x_n, z) = 1.$$

También se puede construir una función recursiva primitiva monádica $U(z)$ tal que si z es el número de Gödel de un protocolo finito de cálculo Z de cierta máquina (reducida) de Turing M, y Z contiene una configuración final K tal que en la cinta K aparece escrito el número natural k, entonces $U(z) = k$. Si en cambio z no tiene la forma indicada, entonces $U(z) = 0$.

Si $P(y, x_1, \ldots, x_s)$ es un predicado recursivo general (en particular, recursivo primitivo), entonces se puede definir una función recursiva parcial $f(x_1, \ldots, x_s)$ mediante la siguiente instrucción: para un conjunto dado $x_1, \ldots, x_s$, comprobamos sucesivamente si son verdaderos o no $P(0, x_1, \ldots, x_s)$, $P(1, x_1, \ldots, x_s)$, $P(2, x_1, \ldots, x_s), \ldots$. En cuanto obtenemos el menor m tal que $P(m, x_1, \ldots, x_s)$ es verdadero, tomamos

$$f(x_1, \ldots, x_s) = m.$$

Si este m no existe, entonces se considera que la función $f(x_1, \ldots, x_s)$ no está definida en el conjunto $x_1, \ldots, x_s$. Esta instrucción se puede expresar como el programa de cierta máquina de Turing y, de esta manera, demostrar la recursividad parcial de f.

Diremos que la función f se obtiene del predicado P mediante la *operación de minimización*, y el valor de $f(x_1, \ldots, x_s)$ se denota con $\mu y P(y, x_1, \ldots, x_s)$ (se lee: «el menor y tal que $P(y, x_1, \ldots, x_s)$»).

Demos un carácter más específico al concepto de sustitución para las funciones parcialmente definidas. Supongamos,

por ejemplo, que g y f son funciones parciales, monádica y s-ádica, respectivamente. Consideremos la función h definida de la siguiente manera: el valor de $h(x_1, \ldots, x_s)$ está definido si y sólo si

1) está definido el valor de $f(x_1, \ldots, x_s)$ y

2) está definido el valor de $g(f(x_1, \ldots, x_s))$ y, en este caso,

$$h(x_1, \ldots, x_s) = g(f(x_1, \ldots, x_s)).$$

En este caso diremos que la función h *se obtiene mediante la sustitución* de la función f en la función g. Esta definición de sustitución para las funciones parciales garantiza que la función h sea recursiva parcial si las funciones f y g también lo son.

La definición de h se puede escribir brevemente en la forma

$$h(x_1, \ldots, x_s) \simeq g(f(x_1, \ldots, x_s)).$$

Aquí y en lo sucesivo, el símbolo $\simeq$ (igualdad condicional) significa que la expresión del primer miembro está definida si y sólo si está definida la expresión del segundo miembro, y si están definidas, entonces ambas expresiones coinciden.

Definamos ahora para cada $n \geqslant 1$ una función recursiva parcial $(n+1)$-ádica $\mathcal{U}_n$ de tal manera que

$$\mathcal{U}_n(e, x_1, \ldots, x_n) \simeq U(\mu z T_n(e, x_1, \ldots, x_n, z)).$$

La propiedad fundamental de $\mathcal{U}_n$ es expresada por el clásico *teorema de la forma normal de Kleene.*

Teorema. *Para toda función recursiva parcial f existe un número natural m tal que, para cualesquiera $x_1, \ldots, x_n$,*

$$f(x_1, \ldots, x_n) \simeq \mathcal{U}_n(m, x_1, \ldots, x_n).$$

► Como m se puede tomar el número de Gödel de la máquina de Turing que calcula la función f. La afirmación se deduce de la definición del predicado T_n y la función f. ◄

Sea K una clase arbitraria de funciones n-ádicas (en general, parciales). La función $g(x, x_1, \ldots, x_n)$ se denomina *función universal para la clase* K si

1) para todo número natural número natural m la función n-ádica respectiva $g(m, x_1, \ldots, x_n)$ pertenece a K;
2) para toda función $f(x_1, \ldots, x_n)$ de K existe un número natural m tal que la función n-ádica $g(m, x_1, \ldots, x_n)$ coincide con f.

El siguiente teorema es consecuencia directa del teorema anterior.

Teorema de la función universal. *Una función recursiva parcial $\mathcal{U}_n$ es universal para la clase de todas las funciones recursivas parciales n-ádicas.*

Veamos un resultado negativo.

Teorema. *No existe una función recursiva parcial $(n+1)$-ádica que sea universal para la clase de todas las funciones recursivas totales n-ádicas.*

► Limitémonos al caso $n = 1$. Supongamos que esta función existe. Denotémosla con $G(x, x_1)$. Puesto que para todo m la función $G(m, x_1)$ es recursiva general, entonces la función $G(x, x_1)$ está definida para cualesquiera x, x_1 y, de esta manera, también es recursiva general. Pero entonces también es recursiva general la función $g(x) = G(x, x) + 1$. Tomemos un m

tal que $g(x) = G(m, x)$. Entonces,

$$G(m, x) = g(x) = G(x, x) + 1.$$

Sustituyendo aquí x por el número m, obtenemos una contradicción. ◄

La idea de esta demostración puede ser utilizada para construir una función recursiva total que no sea recursiva primitiva.

Definamos la función $g(y, x)$ mediante la siguiente instrucción: si y no es el número de Gödel de ninguna descripción RP, entonces $g(y, x) = 0$; si y es el número de Gödel de la descripción RP de la función F, entonces $g(y, x) = F(x)$.

De esta instrucción se puede hacer una máquina de Turing y, de esta manera, demostrar que g es una función recursiva total. Consideremos ahora una función recursiva total F tal que $F(x) = g(x, x) + 1$.

Lema. *La función recursiva total F no es recursiva primitiva.*

► Supongamos lo contrario. Sea m el número de Gödel de la descripción RP de la función F. Entonces,

$$g(m, x) = F(x) = g(x, x) + 1.$$

Sustituyendo aquí x por el número natural m, obtenemos una contradicción. ◄

Para todo número natural m, denotemos con $\{m\}^n$ la correspondiente función recursiva parcial n-ádica

$$U(\mu z T_n(m, x_1, \ldots, x_n, z)).$$

Llamaremos al número m *número de Gödel de la función recursiva parcial* $\{m\}^n$. De esta manera, cada función recursiva parcial

tiene un número de Gödel. El índice n en la notación $\{m\}^n$ se omitirá en algunas ocasiones (confiamos en que el lector no confundirá esta notación tradicional de una función recursiva parcial con la notación de un conjunto unitario en la teoría de conjuntos).

De la definición del predicado T_n se deduce evidentemente que

$$!\{m\}^n(x_1, \ldots, x_n) \Leftrightarrow \exists\, z T_n(m, x_1, \ldots, x_n, z).$$

Recordemos que la expresión de la izquierda significa que la función $\{m\}^n$ está definida en la n-tupla $x_1, \ldots, x_n$.

Lema. *Para todo conjunto recursivamente enumerable A de números naturales, existe una función recursiva parcial g que toma sólo el valor 1 y para todo x*

$$!g(x) \Leftrightarrow x \in A.$$

▶ Si A es recursivamente enumerable, entonces existe una máquina de Turing M que calcula el predicado $x \in A$ de acuerdo con la definición de la subsección 2.3.3. Definamos ahora la función g mediante la siguiente instrucción: $g(x) = 1$ si y sólo si $M(x) = 1$; en todos los demás casos g no está definida. Esta instrucción se puede presentar en forma de una máquina de Turing que calcula g. ◀

Si m es el número de Gödel de la función g indicada en el lema, entonces, evidentemente,

$$x \in A \Leftrightarrow \exists\, z T_1(m, x, z).$$

El número natural m para el que se cumple esta equivalencia se denomina *número de Gödel del conjunto recursivamente enume-*

rable A. Denotemos con $\mathcal{W}_m$ el conjunto recursivamente enumerable con número de Gödel m. De esta manera, por definición,

$$x \in \mathcal{W}_m \Leftrightarrow \exists\, z T_1(m, x, z).$$

2.5.2 Conjuntos y funciones no computables.

Teorema. *El conjunto de números naturales* $\{x \mid \exists\, z T_1,(x,x,z)\}$ *es recursivamente enumerable, pero no es recursivo.*

► La enumerabilidad recursiva del conjunto considerado se deduce del lema de la subsección 2.3.4 y de la recursividad del predicado T_1. Si este conjunto fuera recursivo, entonces su complemento, $A = \{x \mid \neg\exists\, z T_1(x, x, z)\}$, también sería recursivo y, por consiguiente, A sería también recursivamente enumerable. Sin embargo, demostremos que el conjunto A se diferencia de cualquier conjunto recursivamente enumerable. En efecto, consideremos un conjunto recursivamente enumerable arbitrario $\mathcal{W}_m$ y supongamos que $A = \mathcal{W}_m$. Entonces, para todo x,

$$\exists\, z T_1(m, x, z) \Leftrightarrow x \in \mathcal{W}_m \Leftrightarrow x \in A \Leftrightarrow \neg\exists\, z T_1(x, x, z).$$

Sustituyendo en estas equivalencias x por el número m, obtenemos una contradicción. ◄

Corolario. *El conjunto de números naturales*

$$\{x \mid \neg\exists\, z T_1(x, x, z)\}$$

no es recursivamente enumerable.

► De hecho este corolario ya fue demostrado, pero también se puede deducir directamente del teorema anterior y del teorema de Post (véase la subsección 2.3.6). ◄

Corolario. *Existe una función definida en todas partes que es no computable.*

► Definamos la función g de la siguiente manera: para un número natural x, $g(x) = 1$ si $\exists\, zT_1(x, x, z)$, y $g(x) = 0$ si $\neg\exists\, zT_1(x, x, z)$. La función g está definida en todas partes y si ella fuera computable, entonces sería una función recursiva total. Pero $g(x) = 1 \Leftrightarrow \exists\, zT_1(x, x, z)$ y el predicado de la derecha sería recursivo. ◄

2.5.3 Problema de la parada. Diremos que el *problema de la parada* para una máquina de Turing M es *decidible* si existe una función recursiva total h que toma solamente dos valores, 0 y 1, y $h(x) = 1$ si y sólo si la máquina M, al recibir x en la entrada, da un protocolo finito de cálculo.

Hablando informalmente, el problema de la parada es *decidible* si existe un «reconocedor de parada» h capaz de determinar a partir de x si la máquina M se detiene en x o no.

Teorema. *Existe una máquina de Turing M para la que el problema de la parada es indecidible.*

► Sea $a(x)$ una función recursiva total idénticamente igual a cero. Consideremos la función recursiva parcial $g(x)$, que es igual a $a(\mu z T_1(x, x, z))$. Entonces, $!g(x) \Leftrightarrow \exists\, zT_1(x, x, z)$ y $!g(x) \Rightarrow$ $\Rightarrow g(x) = 0$. Supongamos que M' es una máquina de Turing reducida que calcula g. «Modifiquemos» el programa de la máquina M' y obtengamos la máquina M tal que

1) M también calcula g;
2) si para la entrada x la máquina M' da, o bien un protocolo finito de cálculo sin configuración final, o bien un protocolo

finito en cuya configuración final en la cinta está escrita una palabra no vacía, entonces la máquina M no se detiene en la entrada x, es decir, genera un protocolo infinito de cálculos.

Esta modificación de la máquina M' siempre puede ser efectuada agregando algunas instrucciones al final del programa M', variando su estado final y ampliando el alfabeto.

Entonces, $\exists z T_1(x, x, z) \Leftrightarrow M$ se detiene en x. Ahora la imposibilidad de existencia de la correspondiente función h para M se deduce del teorema de la subsección 2.5.2. ◄

Subrayemos que para M es indecidible precisamente el *problema general* de la parada: no existe un algoritmo h *único* que permita determinar si M se detiene en x *para cualquiera que sea* el número natural x. Si se propone un número natural concreto m y se pregunta si es cierto o no que M se detiene para la entrada m, entonces no habrá razones para suponer que es imposible responder a esta pregunta después de reflexionar cierto tiempo. Lo único que es imposible es un método mecánico único de resolución de este problema para cualquier m.

2.5.4 Conjuntos recursivamente inseparables.

Recordemos que con ω se denota el conjunto de todos los números naturales. Dos conjuntos, A_0, $A_1 \subseteq \omega$, se denominan *recursivamente separables* si existen dos conjuntos recursivamente enumerables B_0, B_1 tales que

$$A_0 \subseteq B_0, \quad A_1 \subseteq B_1, \quad B_0 \cap B_1 = \varnothing, \quad B_0 \cup B_1 = \omega.$$

De los conjuntos B_0 y B_1 vamos a decir que ellos *separan recursivamente* los conjuntos A_0 y A_1. Según el teorema de Post

(subsección 2.3.6) los conjuntos B_0 y B_1 son en este caso también recursivos.

Ejercicio. Si los conjuntos A_0, A_1 no son recursivamente separables y no se intersecan (es decir, $A_0 \cap A_1 = \varnothing$), entonces ellos no son recursivos. Más aún, todo conjunto C es tal que $A \subseteq C$, $C \cap B = \varnothing$ tampoco es recursivo.

Definamos dos predicados:

$$W_0(x, y) \rightleftharpoons T_1(j_2 x, x, y) \wedge (\forall\, z \leqslant y) \neg T_1(j_1 x, x, z);$$
$$W_1(x, y) \rightleftharpoons T_1(j_1 x, x, y) \wedge (\forall\, z \leqslant y) \neg T_1(j_2 x, x, z).$$

Se puede demostrar que ambos predicados son recursivos primitivos.

Definamos ahora dos conjuntos recursivamente enumerables:

$$V_0 \rightleftharpoons \{x \mid \exists\, y W_0(x, y)\};$$
$$V_1 \rightleftharpoons \{x \mid \exists\, y W_1(x, y)\}.$$

Teorema. *Los dos conjuntos recursivamente enumerables V_0 y V_1 no se intersecan y no son recursivamente separables.*

▶ Supongamos que $x \in V_0$ y $x \in V_1$. Entonces existen y_0 e y_1 tales que $W_0(x, y_0)$ y $W_1(x, y_1)$, es decir,

1) $T_1(j_2 x, x, y_0)$;
2) $(\forall\, z \leqslant y_0) \neg T_1(j_1 x, x, z)$;
3) $T_1(j_1 x, x, y_1)$;
4) $(\forall\, z \leqslant y_1) \neg T_1(j_2 x, x, z)$.

De 1 y 4 se deduce que $y_1 < y_0$, mientras que de 2 y 3 se deduce que $y_0 < y_1$, es decir, obtenemos una contradicción.

Así pues, los conjuntos V_0 y V_1 no se intersecan.

Consideremos ahora dos conjuntos enumerables arbitrarios B_0, B_1 tales que $V_0 \subseteq B_0$, $V_1 \subseteq B_1$, $B_0 \cap B_1 = \varnothing$, y demostremos que en este caso necesariamente $B_0 \cup B_1 \neq \omega$.

Sean m_0 y m_1 los números de Gödel de B_0 y B_1, respectivamente. Sea $m = j(m_0, m_1)$. Nosotros afirmamos que $m \notin B_0$ y $m \notin B_1$. Demostremos, por ejemplo, que $m \notin B_0$ ($m \notin B_1$ se demuestra de la misma manera).

Supongamos lo contrario: $m \in B_0$. Entonces $m \in \mathscr{W}_{m_0}$, es decir, $\exists y T_1(m_0, m, y)$ y, en virtud de $m_0 = j_1 m$,

$$\exists y T_1(j_1 m, m, y). \tag{1}$$

Luego, en virtud de $m \in B_0$ y $B_0 \cap B_1 = \varnothing$, tenemos

$$m \notin B_1, \tag{2}$$

es decir, $m \notin \mathscr{W}_{m_1}$, lo que significa que $\neg \exists y T_1(m_1, m, y)$, lo que, a su vez, en virtud de $m_1 = j_2 m$, significa

$$\forall y \neg T(j_2 m, m, y). \tag{3}$$

De (1) y (3) se deduce

$$\exists y (T_1(j_1 m, m, y) \wedge (\forall z \leqslant y) \neg T_1(j_2 m, m, z)),$$

es decir, $\exists y W_1(m, y)$ y, por consiguiente, $m \in B_1$. Sin embargo, esto contradice la afirmación (2). ◀

Teorema sobre la función incompletable. *Existe una función recursiva parcial f que toma sólo los valores 0 y 1 para la cual no existe una función recursiva total h que complete f, es decir, no existe una función h tal que para todo x para el cual está definida $f(x)$ se cumpla $f(x) = h(x)$.*

► De acuerdo con el último lema de la subsección 2.5.1 existen dos funciones recursivas parciales g_0 y g_1 tales que $x \in V_i \Leftrightarrow$ $\Leftrightarrow !g_i(x)$. Definamos ahora una función recursiva parcial f mediante la siguiente instrucción: para cada x calculamos $g_0(x)$ y $g_1(x)$. Si $g_0(x)$ está definido, entonces tomamos $f(x) = 0$; si está definido $g_1(x)$, tomamos $f(x) = 1$. Si ambas funciones no están definidas, entonces $f(x)$ se considera no definida. Nótese que los dos valores $g_0(x)$ y $g_1(x)$ no pueden estar definidos al mismo tiempo, ya que $V_0 \cap V_1 = \varnothing$.

Nosotros afirmamos que la función f es la buscada.

Supongamos que una función recursiva total h es la completación recursiva general de la función f. Sea a una función recursiva primitiva tal que $a(0) = 0$, $a(x + 1) = 1$. Definamos $h'(x) = a(h(x))$. Entonces, h' es una función recursiva total que toma sólo los valores 0 y 1 y también completa la función f. Definamos los siguientes conjuntos recursivos:

$$B_0 = \{x \mid h'(x) = 0\}, \quad B_1 = \{x \mid h'(x) = 1\}.$$

De las definiciones se deduce fácilmente que B_0 y B_1 separan recursivamente los conjuntos V_0 y V_1, lo que es imposible debido al teorema anterior. ◄

2.5.5 Teorema de recursión. Tomemos una k-tupla de números naturales,

$$a = \langle e, k_1, \ldots, k_m \rangle,$$

y definamos para ella el número natural t_a de la siguiente manera. Construyamos una máquina de Turing reducida M_a. A saber, para todo conjunto $y_1, \ldots, y_n$ de números naturales el valor

de $M_a(y_1 q \dots y_n q)$ está definido si y sólo si está definida la función universal

$$\mathscr{U}_{m+n}(e, k_1, \dots, k_m, y_1, \dots, y_n),$$

y entonces,

$$M_a(y_1 q \dots q y_n) = \mathscr{U}_{m+n}(e, k_1, \dots, k_m, y_1, \dots, y_n).$$

Tomemos ahora como t_a el número de Gödel de la máquina de Turing M_a.

Nótese ahora que la instrucción ofrece un método para calcular el correspondiente t_a para la tupla a. Esta instrucción puede ser expresada en forma de una máquina de Turing. De esta manera, la función

$$S_n^m(e, x_1, \dots, x_m) = t_{\langle e, x_1, \dots, x_m \rangle}$$

es recursiva general. Un análisis más detallado muestra que S_n^m es incluso una función recursiva primitiva. De esta manera, tiene lugar el siguiente lema.

Lema. *Se puede construir una función recursiva primitiva S_n^m de $(m+1)$ argumentos tal que para todo conjunto de números naturales $e, x_1, \dots, x_m, y_1, \dots, y_n$ tenemos*

$$\{e\}(x_1, \dots, x_m, y_1, \dots, y_n) \simeq$$
$$\simeq \{S_n^m(e, x_1, \dots, x_m)\}(y_1, \dots, y_n).$$

Teorema de recursión de Kleene. *Para toda función recursiva parcial $\psi(z, x_1, \dots, x_n)$ se puede construir un número natural e tal que*

$$\{e\}(x_1, \dots, x_n) \simeq \psi(e, x_1, \dots, x_n).$$

► Consideremos la función recursiva parcial

$$\varphi(y, x_1, \ldots, x_n) \simeq \psi(S_n^1(y, y), x_1, \ldots, x_n).$$

Supongamos que f es su número de Gödel, y $e = S_n^1(f, f)$. Nosotros afirmamos que este número e es el buscado. En efecto,

$$\{e\}(x_1, \ldots, x_n) \simeq \{S_n^1(f, f)\}(x_1, \ldots, x_n) \simeq \{f\}(f, x_1, \ldots, x_n) \simeq$$
$$\simeq \varphi(f, x_1, \ldots, x_n) \simeq \psi(S_n^1(f, f), x_1, \ldots, x_n) \simeq \psi(e, x_1, \ldots, x_n). \quad \blacktriangleleft$$

CAPÍTULO

3

ELEMENTOS DE TEORÍA DE LA DEMOSTRACIÓN

3.1. Incompletitud e indecidibilidad de las teorías axiomáticas 171
3.2. Teorema de Gödel de completitud del cálculo de predicados 187
3.3. Teorema de eliminación del corte 200
3.4. Sobre el programa de Hilbert de fundamentación de la matemática 215

3.1

Incompletitud e indecidibilidad de las teorías axiomáticas

Aquí demostraremos la incompletitud y la indecidibilidad de algunas teorías axiomáticas. La mayor parte de las demostraciones se efectúa para la teoría axiomática concreta Ar^+, pero, como veremos, métodos avanzados serán aplicados también a muchas otras teorías.

3.1.1 Teorema del punto fijo. Recordemos que si A es una palabra sobre un alfabeto simple, entonces con γA denotamos su número de Gödel (subsección 2.4.3). Si m es un número natural, entonces con $\widetilde{m}$, o bien $\tilde{m}$, denotamos un término del lenguaje Ar^+ que naturalmente representa un número natural en el lenguaje Ar^+, es decir, un término de la forma $SS\ldots S0$, donde el símbolo de función S figura m veces (véase la subsección 2.4.6). De esta manera, para toda palabra sobre un alfabeto simple se puede definir un término, la representación natural de esta palabra sobre Ar^+:

$$[A] \leftrightharpoons (\gamma A)\widetilde{\ }.$$

Sean $t(x_1, \ldots, x_n)$ y $r(x_1, \ldots, x_n)$ términos de Ar^+, donde $x_1, \ldots, x_n$ es una lista de diferentes variables entre las que se encuentran todos los parámetros de los términos t y r. Los símbolos de función t y r definen descripciones recursivas primitivas de ciertas funciones recursivas primitivas y, de esta manera, los propios términos definen naturalmente las funciones recursivas primitivas $F(x_1, \ldots, x_n)$ y $G(x_1, \ldots, x_n)$, respectivamente.

Lema. *Para cualesquiera números naturales* $k_1, \ldots, k_n$,

1) *si* $F(k_1, \ldots, k_n) = G(k_1, \ldots, k_n)$, *entonces*

$$\mathrm{Ar}^+ \vdash t(\widetilde{k}_1, \ldots, \widetilde{k}_n) = r(\widetilde{k}_1, \ldots, \widetilde{k}_n);$$

2) *si* $F(k_1, \ldots, k_n) \neq G(k_1, \ldots, k_n)$, *entonces*

$$\mathrm{Ar}^+ \vdash \neg t(\widetilde{k}_1, \ldots, \widetilde{k}_n) = r(\widetilde{k}_1, \ldots, \widetilde{k}_n).$$

Aquí no demostraremos este lema (véase, por ejemplo, [9, 14]). Su esencia radica en que el sistema Ar^+ posee suficientes posibilidades expresivas: todo cálculo recursivo primitivo con números naturales concretos puede ser expresado en Ar^+.

Nótese que no se afirma que, por ejemplo, si $F(k_1, \ldots, k_n) = G(k_1, \ldots, k_n)$ para todos los números naturales $k_1, \ldots, k_n$, entonces $\mathrm{Ar}^+ \vdash t(x_1, \ldots, x_n) = r(x_1, \ldots, x_n)$, con *variables libres* $x_1, \ldots, x_n$. Como veremos posteriormente, esto no es cierto en el caso general. Aquí sólo se afirma la deducibilidad de igualdades formales con *números naturales concretos* $k_1, \ldots, k_n$.

Este lema se denomina *lema de la expresibilidad numérica* de las funciones recursivas primitivas en Ar^+. La palabra «numérica» subraya precisamente que se trata de la deducibilidad

de igualdades numéricas concretas. Si t y r son términos cerrados, entonces en el modelo estándar ω ellos tienen un valor numérico determinado. Del lema anterior se deduce que

$$\text{si} \quad \omega \models t = r, \quad \text{entonces} \quad \mathrm{Ar}^+ \vdash t = r;$$
$$\text{si} \quad \omega \models \neg t = r, \quad \text{entonces} \quad \mathrm{Ar}^+ \vdash \neg t = r.$$

Teorema del punto fijo. *Si A es una fórmula de Ar^+ y x es una variable, entonces se puede construir una fórmula B tal que*

$$\mathrm{Ar}^+ \vdash B \equiv A([B]).$$

Aquí, $A([B]) \leftrightharpoons A(x \parallel [B])$.

► Fijemos la variable x. Tomemos una función recursiva primitiva $\mathrm{SUB}(y, z)$ tal que si y es el número de Gödel de cierta fórmula C, entonces $\mathrm{SUB}(y, z)$ es el número de Gödel de la fórmula $C(x \parallel z)$. La función SUB tiene una descripción recursiva primitiva definida y, por consiguiente, se puede definir el término de la teoría Ar^+ que le corresponde; sea $\mathrm{Sub}(y, z)$ este término.

Para la fórmula dada A, construyamos la fórmula

$$A' \leftrightharpoons A(\mathrm{Sub}(x, x)). \tag{1}$$

y definamos

$$B \leftrightharpoons A'([A']). \tag{2}$$

De aquí se deduce que

$$\gamma B = \mathrm{SUB}(\gamma A', \gamma A').$$

De acuerdo con el lema anterior,

$$\mathrm{Ar}^+ \vdash [B] = \mathrm{Sub}([A'], [A']). \tag{3}$$

A continuación, vemos que en Ar^+ son deducibles las siguientes equivalencias:

$$B \equiv A'([A']) \equiv A'(\mathrm{Sub}([A'], [A'])) \equiv A([B]).$$

La primera equivalencia se deduce de la definición (2) de la fórmula B. La segunda equivalencia tiene lugar en virtud de la definición (1) de la fórmula A'. La tercera equivalencia se deduce de la argumentación (3). ◀

3.1.2 Teorema de incompletitud de Gödel. Con ayuda de la numeración de Gödel, la deducibilidad en la teoría Ar^+ puede ser estudiada dentro de la propia teoría formal Ar^+ (véanse las subsecciones 2.3.7 y 2.4.6). En particular, puede ser construido un predicado recursivo primitivo $\mathrm{PRF}(y, x)$ que es verdadero si y sólo si y es el número de Gödel de una deducción de Ar^+ para la fórmula con número de Gödel x. Como todo predicado recursivo primitivo, él puede ser expresado en la forma $F(y, x) = 1$ para cierta función recursiva primitiva F que toma solamente los valores 0 y 1. Si f es una descripción RP de la función F, entonces al predicado PRF en Ar^+ le corresponde naturalmente la fórmula $f(y, x) = S0$, que denotaremos con $\mathrm{Prf}(y, x)$.

Consideremos ahora la fórmula

$$\mathrm{Pr}(x) \leftrightharpoons \exists\, y\, \mathrm{Prf}(y, x),$$

que afirma que x es el número de Gödel de una fórmula de Ar^+ que es deducible en Ar^+.

Sea A_0 una fórmula concreta cuya negación es deducible en Ar^+. Por ejemplo, como A_0 se puede tomar la fórmula $0 = S0$.

Consideremos la fórmula cerrada

$$\mathrm{Con} \rightleftharpoons \forall y \neg \mathrm{Prf}(y, [0 = S0]).$$

Esta fórmula afirma que la teoría Ar^+ es consistente.

Definamos ahora con ayuda del teorema del punto fijo la *fórmula cerrada de Gödel* ν de tal manera que

$$\mathrm{Ar}^+ \vdash \nu \equiv \neg \mathrm{Pr}([\nu]). \qquad (1)$$

A partir de esta equivalencia, se puede decir que la fórmula ν «afirma que ella misma no es deducible».

Lema 1. *Si la teoría* Ar^+ *es consistente, entonces la fórmula* ν *no es deducible en* Ar^+.

► Supongamos lo contrario; sea p el número de Gödel de una deducción de la fórmula en la teoría Ar^+. Entonces tiene lugar $\mathrm{PRF}(p, \gamma\nu)$ y, según el lema de la subsección 3.1.1, obtenemos $\mathrm{Ar}^+ \vdash \mathrm{Prf}(\widetilde{p}, [\nu])$ y, seguidamente, $\mathrm{Ar}^+ \vdash \mathrm{Pr}([\nu])$, lo que en virtud de (1) implica $\mathrm{Ar}^+ \vdash \neg\nu$. Por otra parte, según la suposición, $\mathrm{Ar}^+ \vdash \nu$, y llegamos a la conclusión de que la teoría Ar^+ es contradictoria, lo que contradice lo supuesto. ◄

Nota. Recordemos que una teoría T se denomina *consistente* si no existe una fórmula A de la teoría T tal que simultáneamente $T \vdash A$ y $T \vdash \neg A$. Una teoría T es consistente si y sólo si existe una fórmula que no es deducible en T. El lector podría pensar que la exigencia de la consistencia de la teoría en el enunciado del lema anterior está de más. Parece evidente que esta condición de todos modos se cumple. La teoría Ar^+ es, por supuesto, consistente. En efecto, todas las fórmulas deducibles en Ar^+ son verdaderas en el modelo estándar ω, mientras que, por ejemplo, la fórmula $0 = S0$ es falsa en el modelo estándar y, por consiguiente, no es deducible en Ar^+.

La cuestión radica en que quisiéramos que tanto la formulación como la demostración del lema 1 se formalicen naturalmente en la teoría Ar^+, y, como veremos más adelante, precisamente la fórmula Con no es deducible en Ar^+. La demostración de la consistencia de Ar^+ esbozada por nosotros utiliza algunos razonamientos teórico-conjuntistas de la teoría de modelos y no puede ser traducida directamente al lenguaje Ar^+.

Sea T una teoría en el lenguaje Ar^+. Diremos que T es una *teoría ω-consistente* si no existe una fórmula $A(y)$ con una variable libre tal que

1) $T \vdash \exists y A(y)$;
2) para todo número natural m tiene lugar $T \vdash \neg A(\widetilde{m})$.

Ejercicio. Demostrar que si T es *ω-consistente*, entonces la teoría T también es consistente.

Lema 2. *Si Ar^+ es ω-consistente, entonces en Ar^+ la fórmula $\neg\nu$ no es deducible.*

► Supongamos lo contrario: $\mathrm{Ar}^+ \vdash \neg\nu$. De acuerdo con (1), $\mathrm{Ar}^+ \vdash \mathrm{Pr}([\nu])$, es decir, $\mathrm{Ar}^+ \vdash \exists y \mathrm{Prf}(y, [\nu])$. Por otra parte, tomemos un número natural arbitrario m. Tenemos $\neg\mathrm{PRF}(m, \gamma\nu)$, puesto que, de acuerdo con el lema 1, la fórmula ν no es deducible. Según el lema de la subsección 3.1.1, de aquí resulta $\mathrm{Ar}^+ \vdash \neg\mathrm{Prf}(\widetilde{m}, [\nu])$, y obtenemos una ω-contradicción en Ar^+. ◄

Teorema de incompletitud de Gödel. *Si la teoría Ar^+ es ω-consistente, entonces la fórmula ν y la fórmula $\neg\nu$ no son deducibles en esta teoría.*

► Este teorema es una consecuencia de los lemas 1 y 2. ◄

Nota. Recordemos que una teoría es completa si para toda fórmula cerrada A tenemos, o bien $T \vdash A$, o bien $T \vdash \neg A$. Resulta que la teoría Ar^+ es incompleta.

La fórmula ν es verdadera en el modelo estándar ω, ya que, en virtud del lema 1, no existe una deducción de ν en Ar^+ y, por consiguiente, es verdadera la fórmula $\neg\mathrm{Pr}([\nu])$. De esta manera, ν es un ejemplo de sentencia verdadera que no es deducible en Ar^+.

No es cierto que $\mathrm{Ar}^+ \vdash \neg\mathrm{Prf}(y, [\nu])$ con variable libre y, puesto que de otro modo podríamos fácilmente obtener $\mathrm{Ar}^+ \vdash \nu$. No obstante, para todo número natural concreto m tenemos $\mathrm{Ar}^+ \vdash \neg\mathrm{Prf}(\widetilde{m}, [\nu])$. Es como si a la teoría Ar^+ no tuviera «abstracción generalizadora», lo que motiva su incompletitud.

Consideremos la teoría $T = \mathrm{Ar}^+ + \neg\nu$, que se obtiene añadiendo a Ar^+ como nuevo axioma no lógico la proposición (falsa) $\neg\nu$. La teoría T es consistente, puesto que si en T se dedujera una contradicción, entonces, de acuerdo con las leyes de la lógica, $\mathrm{Ar}^+ \vdash \nu$. Sin embargo, la teoría T es ω-contradictoria. En efecto, $\neg\nu$ es equivalente a $\exists\, y\mathrm{Prf}(y, [\nu])$, de modo que $T \vdash \exists\, y\mathrm{Prf}(y, [\nu])$. Por otro lado, para todo número natural m, de acuerdo con el lema 1, $\neg\mathrm{PRF}(m, \gamma\nu)$ y, por tanto, en Ar^+, y con mayor razón en T, es deducible $\neg\mathrm{Prf}(\widetilde{m}, [\nu])$.

3.1.3 Segundo teorema de Gödel. Tanto la formulación como la demostración del lema 1 de la subsección anterior se refieren solamente a objetos constructivos y, luego de pasar a los números de Gödel, admiten una formalización natural dentro de la teoría Ar^+. Después de realizar esta formalización, obte-

nemos la siguiente afirmación:

$$\mathrm{Ar}^+ \vdash \mathrm{Con} \supset \neg\mathrm{Pr}([\nu]).$$

Luego, tiene lugar la siguiente afirmación :

$$\neg\exists\, y\mathrm{PRF}(y, \gamma\nu) \Rightarrow (\mathrm{Ar}^+ \textit{ es consistente}).$$

► En efecto, supongamos que Ar^+ es contradictoria. Entonces, en Ar^+ es deducible cualquier fórmula y, en particular, ν. Si D es una deducción de ν en Ar^+, entonces tiene lugar $\mathrm{PRF}(\gamma D, \gamma\nu)$ y, por consiguiente, $\exists\, y\mathrm{PRF}(y, \gamma\nu)$, lo que contradice la suposición hecha. ◄

Esta demostración admite una formalización simple en la teoría Ar^+, como resultado de lo cual obtenemos la afirmación

$\mathrm{Ar}^+ \vdash \neg\exists\, y\mathrm{Prf}(y, [\nu]) \supset \mathrm{Con}$, es decir, $\mathrm{Ar}^+ \vdash \neg\mathrm{Pr}([\nu]) \supset \mathrm{Con}$.

Confrontando las dos argumentaciones obtenidas, concluimos que

$$\mathrm{Ar}^+ \vdash \neg\mathrm{Pr}([\nu]) \equiv \mathrm{Con}.$$

Por otra parte, según la construcción de ν, tenemos

$$\mathrm{Ar}^+ \vdash \nu \equiv \neg\mathrm{Pr}([\nu]).$$

De esta manera, finalmente,

$$\mathrm{Ar}^+ \vdash \mathrm{Con} \equiv \nu.$$

Teorema (segundo teorema de Gödel). *Si la teoría* Ar^+ *es consistente, entonces la fórmula* Con *no es deducible en* Ar^+.

► Este teorema es consecuencia de la argumentación anterior y el lema 1 de la subsección anterior. ◄

El segundo teorema de Gödel expresa un resultado de importancia fundamental: la consistencia de la teoría considerada no puede ser demostrada con ayuda de medios de la propia teoría. Para demostrar la consistencia de una teoría es necesario utilizar conceptos que se encuentran fuera esta teoría. Precisamente de esta manera se logró demostrar la consistencia de la teoría Ar^+, utilizando razonamientos de la teoría de modelos. De manera análoga se puede demostrar que la consistencia de ZF no puede ser obtenida en el marco de la propia teoría ZF. Un problema sumamente interesante es la búsqueda de medios suficientemente convincentes que salen de los límites de ZF.

3.1.4 Teorema de incompletitud en la forma de Rosser.

Como demostró Rosser, si se elige de manera adecuada una fórmula, en el teorema de incompletitud se puede reemplazar la ω-consistencia por la consistencia, que es una exigencia más débil.

Consideremos una función recursiva primitiva $\mathrm{NEG}(x)$ tal que si x es el número de Gödel de una fórmula A, entonces $\mathrm{NEG}(x)$ es el número de Gödel de la fórmula $\neg A$. Según la descripción recursiva primitiva de esta función, se puede construir el correspondiente término $\mathrm{Neg}(x)$ de la teoría Ar^+.

Construyamos con ayuda del teorema del punto fijo una fórmula ρ de manera que

$$\mathrm{Ar}^+ \vdash \rho \equiv \forall y(\mathrm{Prf}(y, [\rho]) \supset (\exists z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))).$$

Teorema de incompletitud de Rosser. *Si la teoría* Ar^+ *es consistente, entonces en ella no son deducibles ni la fórmula* ρ, *ni la fórmula* $\neg\rho$.

► Supongamos que $\mathrm{Ar}^+ \vdash \rho$. Entonces existe un m tal que $\mathrm{PRF}(m, \gamma\rho)$. Si para cierto i tuviéramos $\mathrm{PRF}(i, \gamma(\neg\rho))$, entonces la teoría Ar^+ sería contradictoria, lo que contradice la condición.

De este modo, tenemos

$$\mathrm{PRF}(m, \gamma\rho) \wedge (\forall\, z \leqslant m)\neg\mathrm{PRF}(z, \mathrm{NEG}(\gamma\rho)).$$

Esta relación recursiva primitiva puede ser deducida en Ar^+; obtenemos

$$\mathrm{Ar}^+ \vdash \mathrm{Prf}(\widetilde{m}, [\rho]) \wedge (\forall\, z \leqslant \widetilde{m})\neg\mathrm{Prf}(z, \mathrm{Neg}([\rho])).$$

De aquí

$$\mathrm{Ar}^+ \vdash \exists\, y(\mathrm{Prf}(y, [\rho]) \wedge (\forall\, z \leqslant y)\neg\mathrm{Prf}(z, \mathrm{Neg}([\rho])).$$

Pero esta fórmula es lógicamente equivalente a $\neg\rho$. De esta manera, $\mathrm{Ar}^+ \vdash \rho$, lo que contradice la suposición $\mathrm{Ar}^+ \vdash \rho$.

Supongamos ahora que $\mathrm{Ar}^+ \vdash \neg\rho$. Entonces existe un número natural m tal que $\mathrm{PRF}(m, \mathrm{NEG}(\gamma\rho))$ y, según el lema de la subsección 3.1.1, $\mathrm{Ar}^+ \vdash \mathrm{Prf}(\widetilde{m}, \mathrm{Neg}([\rho]))$.

De aquí, de acuerdo con las leyes de la aritmética formal, obtenemos

$$\mathrm{Ar}^+ \vdash (\forall\, y \geqslant \widetilde{m})(\exists\, z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]));$$

debilitando esta afirmación, resulta

$$\mathrm{Ar}^+ \vdash (\forall\, y \geqslant \widetilde{m})(\mathrm{Prf}(y, [\rho]) \supset (\exists\, z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))). \qquad (1)$$

Aparte de esto, tiene lugar la afirmación informal

$$(\forall\, y \leqslant m)(\mathrm{PRF}(y, \gamma[\rho]) \Rightarrow (\exists\, z \leqslant y)\mathrm{PRF}(z, \mathrm{NEG}(\gamma\rho))), \qquad (2)$$

simplemente en virtud de que para todo y el predicado $\mathrm{PRF}(y, \gamma\rho)$ es falso (ya que de otro modo tendríamos $\mathrm{Ar}^+ \vdash \rho$, y la teoría Ar^+ sería contradictoria).

La relación recursiva primitiva (2) puede ser deducida en Ar^+; por tanto,

$$\mathrm{Ar}^+ \vdash (\forall\, y \leqslant \widetilde{m})(\mathrm{Prf}(y, [\rho]) \supset (\exists\, z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))). \qquad (3)$$

Comparando (1) y (3), de acuerdo con las leyes de la aritmética formal, obtenemos

$$\mathrm{Ar}^+ \vdash \forall\, y(\mathrm{Prf}(y, [\rho]) \supset (\exists\, z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))),$$

lo que es $\mathrm{Ar}^+ \vdash \rho$. De esta manera, $\mathrm{Ar}^+ \vdash \rho$ y $\mathrm{Ar}^+ \vdash \neg\rho$, y obtenemos nuevamente una contradicción. ◄

3.1.5 Teorema de Löb. *Si* $\mathrm{Ar}^+ \vdash \mathrm{Pr}([A]) \supset A$, *entonces* $\mathrm{Ar}^+ \vdash A$.

► De acuerdo con el teorema del punto fijo, existe una fórmula ψ tal que

$$\mathrm{Ar}^+ \vdash \psi \equiv (\mathrm{Pr}([\psi]) \supset A). \qquad (1)$$

Lema. $\mathrm{Ar}^+ \vdash \psi \Rightarrow \mathrm{Ar}^+ \vdash A$.

► Supongamos que $\mathrm{Ar}^+ \vdash \psi$. Sea m la correspondiente deducción. Entonces, $\mathrm{PRF}(m, \gamma\psi)$ y, por tanto, $\mathrm{Ar}^+ \vdash \mathrm{Prf}(\widetilde{m}, [\psi])$; de aquí, $\mathrm{Ar}^+ \vdash \mathrm{Pr}([\psi])$. En virtud de (1), tenemos $\mathrm{Ar}^+ \vdash \psi \equiv A$. Según la suposición, de aquí resulta $\mathrm{Ar}^+ \vdash A$. ◄

Si formalizamos la demostración de este lema, obtendremos

$$\mathrm{Ar}^+ \vdash \mathrm{Pr}([\psi]) \supset \mathrm{Pr}([A]). \qquad (2)$$

Luego, de acuerdo con la suposición del teorema, tenemos

$$\mathrm{Ar}^+ \vdash \mathrm{Pr}([A]) \supset A. \tag{3}$$

De (2) y (3), resulta

$$\mathrm{Ar}^+ \vdash \mathrm{Pr}([\psi]) \supset A,$$

lo que en virtud de (1) nos da $\mathrm{Ar}^+ \vdash \psi$. Entonces, de acuerdo con el lema, tenemos $\mathrm{Ar}^+ \vdash A$. ◄

3.1.6 Indecidibilidad. Denotemos con $[\mathrm{Ar}^+]^0$ el conjunto de todos los números de Gödel de las sentencias deducibles en Ar^+, y con $[\mathrm{Ar}^+]^1$, el conjunto de todos los números de Gödel de las sentencias refutables en Ar^+, es decir,

$$[\mathrm{Ar}^+]^1 \leftrightharpoons \{\gamma B \mid \mathrm{Ar}^+ \vdash \neg B, B \text{ es una sentencia}\}.$$

Teorema. *Los conjuntos* $[\mathrm{Ar}^+]^0$ *y* $[\mathrm{Ar}^+]^1$ *de los números de las sentencias deducibles y refutables, respectivamente, de* Ar^+ *no son recursivamente separables.*

► Tomemos dos predicados recursivos primitivos, $W_0(x, y)$ y $W_1(x, y)$ (véase la subsección 2.5.4). Ellos se definen mediante fórmulas aritméticas que denotaremos con W_0 y W_1. Como se demostró en el segundo capítulo, los conjuntos

$$V_0 = \{x \mid \exists\, y W_0(x, y)\} \quad \text{y} \quad V_1 = \{x \mid \exists\, y W_1(x, y)\}$$

no se intersecan, es decir,

$$\exists\, y W_1(x, y) \Rightarrow \neg \exists\, y W_0(x, y).$$

La demostración de esta afirmación se puede formalizar en Ar^+ y obtener

$$\mathrm{Ar}^+ \vdash \exists\, y W_1(x, y) \supset \neg \exists\, y W_0(x, y). \tag{1}$$

Definamos ahora la fórmula $B(x) \leftrightharpoons \exists y W_0(x, y)$.

Si $m \in V_0$, entonces existe un k tal que $W_0(m, k)$, es decir, $\mathrm{Ar}^+ \vdash W_0(\widetilde{m}, \widetilde{k})$; por consiguiente, $\mathrm{Ar}^+ \vdash \exists y W_0(\widetilde{m}, y)$, es decir, $\mathrm{Ar}^+ \vdash B(\widetilde{m})$ y, por tanto, $\gamma B(\widetilde{m}) \in [\mathrm{Ar}^+]^0$. Así pues,

$$m \in V_0 \Rightarrow \gamma B(\widetilde{m}) \in [\mathrm{Ar}^+]^0. \tag{2}$$

Supongamos ahora que $m \in V_1$. Entonces, existe un k tal que $W_1(m, k)$. De aquí, $\mathrm{Ar}^+ \vdash W_1(\widetilde{m}, \widetilde{k})$ y, seguidamente, $\mathrm{Ar}^+ \vdash \vdash \exists y W_1(\widetilde{m}, y)$. Entonces, en virtud de (1), $\mathrm{Ar}^+ \vdash \neg \exists y W_0(\widetilde{m}, y)$, es decir, $\mathrm{Ar}^+ \vdash \neg B(\widetilde{m})$ y, de esta manera, $B(\widetilde{m}) \in [\mathrm{Ar}^+]^1$. Así pues,

$$m \in V_1 \Rightarrow \gamma B(\widetilde{m}) \in [\mathrm{Ar}^+]^1. \tag{3}$$

Supongamos lo contrario: B_0 y B_1 separan recursivamente los conjuntos $[\mathrm{Ar}^+]^0$, $[\mathrm{Ar}^+]^1$, es decir, B_0 y B_1 son recursivamente enumerables,

$$[\mathrm{Ar}^+]^0 \subseteq B_0, [\mathrm{Ar}^+]^1 \subseteq B_1, \tag{4}$$

$$B_0 \cap B_1 = \varnothing, B_0 \cup B_1 = \omega. \tag{5}$$

Definamos entonces los conjuntos recursivamente enumerables $B_i' = \{m \mid \gamma B(\widetilde{m}) \in B_i\}$. En virtud de (2)–(4), tenemos $V_i \subseteq B_i'$, y en virtud de (5), $B_0' \cap B_1' = \varnothing$, $B_0' \cup B_1' = \omega$. De esta manera, los conjuntos V_0, V_1 son también recursivamente separables, lo que es imposible. ◄

Teorema de la indecidibilidad. *Sea T una teoría consistente en el lenguaje Ar^+ en la cual se deducen todos los axiomas no lógicos de Ar^+. Entonces, T es indecidible.*

► Todo lo que se puede deducir en Ar^+, se puede deducir también en T, de modo que $[T]^0 \subseteq [\mathrm{Ar}^+]^0$. En virtud de la

consistencia de T, es evidente que $[T]^0 \cap [\mathrm{Ar}^+]^1 = \varnothing$. Si la teoría T fuera decidible, entonces el conjunto $[T]^0$ sería recursivo. En este caso, también sería recursivo el complemento de este conjunto, $\omega \setminus [T]^0$. Pero entonces los conjuntos $[T]^0$ y $\omega \setminus [T]^0$ separan recursivamente los conjuntos $[\mathrm{Ar}^+]^0$ y $[\mathrm{Ar}^+]^1$. ◄

Corolario. *Si* Ar^+ *es consistente, entonces* Ar^+ *es una teoría indecidible.*

► Es suficiente tomar en el teorema Ar^+ como T. ◄

3.1.7. Generalización de los resultados a otras teorías. Hemos investigado detalladamente sólo la teoría Ar^+, pero todos los teoremas de la presente sección son válidos para otras teorías. Es suficiente que la teoría considerada T posea las dos propiedades siguientes:

1) La teoría debe ser explícitamente definida. Esto es necesario para que se pueda hablar en el lenguaje de la aritmética sobre la deducibilidad en esta teoría, por ejemplo, para que exista un predicado recursivo general $\mathrm{PRF}_T(y, x)$ y se pueda construir la correspondiente fórmula aritmética $\mathrm{Prf}_T(y, x)$, que afirme que y es el número de Gödel de la deducción en la teoría T de la fórmula con número de Gödel x.

2) La teoría T debe contener la aritmética Ar^+. Esto es necesario para que en el marco de la teoría T se puedan deducir las propiedades necesarias de los predicados aritméticos y, por tanto, demostrar en T las propiedades necesarias del predicado de deducibilidad de la propia teoría T. El concepto «contener la aritmética» puede interpretarse en este caso de manera muy amplia. Es suficiente que, en uno u otro sentido, la teoría Ar^+

se interprete en la teoría T; por ejemplo, es suficiente que exista cierta traducción A^0 de las fórmulas del lenguaje Ar^+ en las fórmulas de la teoría T, una traducción que posea propiedades análogas a las indicadas en la subsección 2.4.7.

Las teorías Ar, Ar^+, Ar2 y ZF satisfacen estas exigencias. Por consiguiente, si estas teorías son consistentes, entonces ellas son incompletas, indecidibles y los conjuntos de sus sentencias deducibles y refutables no son recursivamente separables. Para cada una de las teorías indicadas T, se puede considerar la fórmula aritmética Con$T$, que afirma que la teoría T es consistente:

$$\mathrm{Con}T \leftrightharpoons \neg\exists\, y \mathrm{Prf}_T(y, [A_0]),$$

donde A_0 es una proposición fija de T cuya negación es deducible es T.

Si la teoría T es consistente, entonces la fórmula Con$T$ (más exactamente, su traducción a la teoría T) no se deduce en T. En esto consiste el segundo teorema de Gödel, formulado en el caso de la teoría T.

En lo sucesivo no nos dedicaremos al análisis de la clase de las teorías para las que se cumplen estos teoremas; sólo mencionaremos un resultado clásico más.

Un análisis cuidadoso muestra que el resultado sobre la indecidibilidad de Ar^+, dado en la subsección 3.1.6, se obtiene si en lugar de toda la teoría Ar^+ se toma sólo el fragmento Ar^- de la teoría Ar que contiene sólo un número finito de axiomas no lógicos de Ar. Denotemos la conjunción de todos los axiomas de Ar^- con A. Ésta es una sentencia del lenguaje Ar. De la definición de deducibilidad se obtiene que

$$\mathrm{Ar}^- \vdash B \Leftrightarrow \vdash A \supset B,$$

donde a la derecha se tiene una argumentación en la lógica de predicados.

Teorema de indecidibilidad del cálculo de predicados. *El conjunto de las fórmulas deducibles en el cálculo de predicados (en el lenguaje* Ar*) no es recursivo.*

► Supongamos que este conjunto es recursivo. Entonces existe una función recursiva total f tal que $f(\gamma B) = 1 \Leftrightarrow \vdash B$ para toda fórmula B. Definamos la función recursiva total h mediante la siguiente instrucción: $h(x)$ es igual, o bien a 0, o bien a 1, y $h(x) = 1 \Leftrightarrow x$ es el número de Gödel de cierta fórmula B del lenguaje Ar, y $f(\gamma(A \supset B)) = 1$. Entonces,

$$h(\gamma B) = 1 \Leftrightarrow \mathrm{Ar}^{-} \vdash B,$$

y la teoría Ar^{-} resulta decidible. ◄

3.2 Teorema de Gödel de completitud del cálculo de predicados

3.2.1 No es difícil comprobar que toda fórmula deducible en el cálculo de predicados es una tautología, es decir, una ley lógica. El teorema de completitud de Gödel afirma que el recíproco es válido, es decir, toda ley lógica necesariamente se deduce en el cálculo de predicados. De esta manera, el cálculo de predicados es un instrumento adecuado para la obtención de leyes lógicas.

Recordemos que una teoría T en un lenguaje Ω se denomina *consistente* si no existe una fórmula C del lenguaje Ω tal que

$$T \vdash C \quad \text{y} \quad T \vdash \neg C.$$

El resultado principal de esta sección es el siguiente teorema fundamental sobre la existencia de un modelo. Este teorema también fue demostrado, en esencia, por Gödel.

Teorema. *Toda teoría consistente T en un lenguaje Ω de primer orden tiene un modelo.*

► Sea Ω un lenguaje de primer orden. Supongamos que T es una teoría axiomática formal consistente en el lenguaje Ω. Construiremos un modelo M para la teoría T.

Nos limitaremos al caso cuando el lenguaje Ω sólo contiene un conjunto numerable o finito de símbolos. Este teorema es válido para cualquier lenguaje de primer orden, y el método de demostración, en lo fundamental, es el mismo, pero aparece la necesidad de utilizar algunos medios específicos de la teoría de conjuntos (por ejemplo, la llamada *inducción transfinita*).

Sea X el conjunto de todos los axiomas no lógicos de la teoría T.

Tomemos un conjunto numerable V de constantes que no forman parte del lenguaje Ω, y consideremos el lenguaje Ψ que se obtiene si a Ω se le agrega el conjunto V como conjunto de nuevas constantes. Denotemos con St_Ψ el conjunto de todas las sentencias del lenguaje Ψ. Fijemos una proposición C del lenguaje Ω y definamos $\top \leftrightharpoons C \vee \neg C$ y $\bot \leftrightharpoons C \wedge \neg C$. Sean Γ y Δ conjuntos finitos de fórmulas del lenguaje Ψ, $\Gamma = \{A_1, \ldots, A_m\}$, $\Delta = \{B_1, \ldots, B_k\}$. Denotemos con $\Gamma \to \Delta$ la fórmula

$$\top \wedge\ A_1 \wedge \ldots \wedge A_m \supset B_1 \vee \ldots \vee B_k \vee \bot.$$

Si $k > 0$, $m > 0$, entonces esta fórmula es equivalente a $A_1 \wedge \wedge \ldots \wedge A_m \supset B_1 \vee \ldots \vee B_k$. Si $m > 0$, $k = 0$, entonces $\Gamma \to \Delta$ es equivalente a $\neg(A_1 \wedge \ldots \wedge A_m)$. Si $m = 0$, $k > 0$, esta fórmula es equivalente a $B_1 \vee \ldots \vee B_k$. Finalmente, para $m = 0$, $k = 0$, esta fórmula es equivalente a $\bot$.

Un par de conjuntos $Y, Z \subseteq \mathrm{St}_\Psi$ se denomina *compatible* si para cualesquiera conjuntos finitos $\Gamma \subseteq Y$, $\Delta \subseteq Z$ la fórmula $\Gamma \to \Delta$ no es deducible en el cálculo de predicados.

Un par de conjuntos $Y, Z \subseteq \mathrm{St}_\Psi$ se denomina *completo* si

1) $(A \wedge B) \in Y \Rightarrow A \in Y$ y $B \in Y$;
2) $(A \wedge B) \in Z \Rightarrow A \in Z$ o $B \in Z$;
3) $(A \vee B) \in Y \Rightarrow A \in Y$ o $B \in Y$;
4) $(A \vee B) \in Z \Rightarrow A \in Z$ y $B \in Z$;
5) $(A \supset B) \in Y \Rightarrow A \in Z$ o $B \in Y$;
6) $(A \supset B) \in Z \Rightarrow A \in Y$ y $B \in Z$;
7) $\neg A \in Y \Rightarrow A \in Z$;
8) $\neg A \in Z \Rightarrow A \in Y$;
9) $\forall x A(x) \in Y \Rightarrow$ para todo término cerrado t del lenguaje Ψ $A(t) \in Y$;
10) $\exists x A(x) \in Z \Rightarrow$ existe una constante $c \in V$, $A(c) \in Z$;
11) $\exists x A(x) \in Y \Rightarrow$ existe una constante $c \in V$, $A(c) \in Y$;
12) $\exists x A(x) \in Z \Rightarrow$ para todo término cerrado T del lenguaje Ψ $A(t) \in Z$.

Lema. *Existe un par completo y compatible de conjuntos Y, Z tal que $X \subseteq Y$.*

► Construyamos los conjuntos Y, Z gradualmente. En cada etapa obtendremos conjuntos Y_n, Z_n, y definiremos

$$Y = \bigcup_{n \in \omega} Y_n \quad \text{y} \quad Z = \bigcup_{n \in \omega} Z_n.$$

Al pasar a la etapa siguiente, aumentaremos la cantidad de fórmulas, de modo que $Y_n \subseteq Y_{n+1}$ y $Z_n \subseteq Z_{n+1}$. La agregación de fórmulas se realiza de manera que se garantiza el cumplimiento de las condiciones de completitud 1–12 para los conjuntos finales Y, Z. Para procesar sistemáticamente todas las fórmulas que forman parte de Y_n, Z_n, es conveniente numerar

las fórmulas con números naturales y considerarlas según el orden de sus números.

Pasemos ahora a las definiciones exactas. Un *conjunto numerado de fórmulas* es, por definición, un conjunto F de pares de la forma $\langle n, A\rangle$, donde n es un número natural y A es una sentencia del lenguaje Ψ. Se cumplen las siguientes condiciones:

a) $\langle n, A\rangle \in F$, $\langle n, B\rangle \in F \Rightarrow A = B$;

b) existe sólo un número finito de n impares tales que $\langle n, A\rangle \in F$.

Si $\langle n, A\rangle \in F$, entonces el número n se denomina *orden* de la fórmula A en el conjunto F. Según las condiciones, el orden define completamente la fórmula A en F. Además, sólo un número finito de fórmulas tiene orden impar.

Para el conjunto numerado F, se puede formar el conjunto de fórmulas

$$F' = \{A \in \mathrm{St}_\Psi \mid (\exists\, n \in \omega)(\langle n, A\rangle) \in F)\}.$$

Un *par numerado de conjuntos* es, por definición, un par de conjuntos numerados F, G tal que de $\langle n, A\rangle \in F$, $\langle m, B\rangle \in G$ se deduce $n \neq m$. En este caso, $F \cup G$ es un conjunto numerado. El elemento $\langle n, A\rangle \in F \cup G$ de orden menor será llamado *elemento de turno* en F, G. El *peso* del par F, G es un número natural h definido de la siguiente manera. Si $F \cup G$ no contiene elementos de orden impar, entonces $h = 0$. Si $2k - 1$ es el mayor orden impar en $F \cup G$, entonces tomamos $h = k$. De esta manera, si h es el peso de F, G, entonces $F \cup G$ no contiene elementos de órdenes $2h + 1, 2h + 3, \ldots$.

Numeremos todos los términos cerrados del lenguaje Ψ en una sucesión única:

$$t_1, t_2, \ldots, t_n \ldots.$$

Hagamos lo mismo con las constantes de V:

$$c_1, c_2, \ldots, c_n \ldots.$$

Comencemos la demostración del lema. Construyamos un par numerado F_1, G_1 tal que $F_1' = X, G_1' = \{C \wedge \neg C\}$, numerando todas las fórmulas de F_1', G_1' con números *pares*. El peso h_1 de este par es igual a cero. Además, ninguna de las fórmulas de $F_1' \cup G_1'$ contiene constantes de V, puesto que ella pertenece al lenguaje Ω. El par de conjuntos F_1', G_1' es compatible, ya que el conjunto X es consistente.

Definamos inductivamente la sucesión de pares numerados F_1, G_1; F_2, G_2; ...; F_n, G_n; ... de manera que cada conjunto de fórmulas $F_n' \cup G_n'$ contenga sólo un conjunto finito de constantes de V y el par F_n', G_n' sea compatible. Denotemos con h_n el peso de F_n, G_n.

Supongamos que el par F_n, G_n ya ha sido construido. Indiquemos cómo se debe definir el par F_{n+1}, G_{n+1}. Sea $\langle m, A\rangle$ el *elemento de turno* del par F_n, G_n. Eliminemos el elemento $\langle m, A\rangle$ del conjunto (F_n o G_n) del cual $\langle m, A\rangle$ forma parte, e introduzcamos en este conjunto el nuevo elemento $\langle 2h_n + 1, A\rangle$. Denotemos el par obtenido con P_n, Q_n. Evidentemente,

$$P_n' = F_n', \quad Q_n' = G_n'.$$

Analicemos ahora los casos posibles en dependencia de la forma del elemento $\langle m, A\rangle$.

1) $\langle m, A\rangle \in F_n$, $A = A_1 \wedge A_2$.

Entonces,

$$F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1\rangle, \quad \langle 2h_n + 5, A_2\rangle\}, \quad G_{n+1} = Q_n.$$

El par F'_{n+1}, G'_{n+1} es compatible, puesto que en caso contrario existirían conjuntos finitos $\Gamma \subseteq F'_n, \Delta \subseteq G'_n$ tales que $\vdash \{A_1, A_2\} \cup \Gamma \to \Delta$. Entonces, de acuerdo con las reglas del cálculo de predicados, $\vdash \{A_1 \wedge A_2\} \cup \Gamma \to \Delta$ y, puesto que $A_1 \wedge A_2 \in F'_n$, el par F'_n, G'_n resultaría incompatible.

2) $\langle m, A\rangle \in G_n$, $A = A_1 \wedge A_2$.

Uno de los pares, o bien

$$F'_n, G'_n \cup \{A_1\},$$

o bien

$$F'_n, G'_n \cup \{A_2\}$$

es necesariamente compatible. En efecto, de lo contrario existirían conjuntos finitos $\Gamma \subseteq F'_n$ y $\Delta \subseteq G'_n$ tales que $\vdash \Gamma \to \Delta \cup \{A_1\}$ y $\vdash \Gamma \to \Delta \cup \{A_2\}$. Entonces, de acuerdo con las reglas del cálculo de predicados, $\vdash \Gamma \to \Delta \cup \{A_1 \wedge A_2\}$, puesto que $A_1 \wedge A_2 \in G'_n$, y el par F'_n, G'_n resultaría incompatible. Supongamos que es compatible el par $F'_n, G'_n \cup \{A_i\}$. Tomamos

$$F_{n+1} = P_n, \quad G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_i\rangle\}.$$

3) $\langle m, A\rangle \in F_n$, $A = A_1 \vee A_2$.

Uno de los pares, o bien

$$\{A_1\} \cup F'_n, G'_n,$$

o bien

$$\{A_2\} \cup F'_n, G'_n$$

es necesariamente compatible. En efecto, de lo contrario existirían conjuntos finitos Γ y Δ, $\Gamma \subseteq F'_n, \Delta \subseteq G'_n$, tales que $\vdash \{A_1\} \cup \Gamma \to \Delta$ y $\vdash \{A_2\} \cup \Gamma \to \Delta$. Entonces, $\vdash \{A_1 \vee A_2\} \cup \Gamma \to \Delta$, y el par F'_n, G'_n resultaría incompatible. Supongamos que es compatible

el par $\{A_i\} \cup F'_n, G'_n$. Tomamos $F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_i\rangle\}$, $G_{n+1} = Q_n$.

4) $\langle m, A\rangle \in G_n$, $A = A_1 \vee A_2$.

Entonces

$$F_{n+1} = P_n, \quad G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_1\rangle, \quad \langle 2h_n + 5, A_2\rangle\}.$$

5) $\langle m, A\rangle \in F_n$, $A = A_1 \supset A_2$.

Uno de los pares, o bien

$$\{A_2\} \cup F'_n, G'_n,$$

o bien

$$F'_n, G'_n \cup \{A_1\}$$

es necesariamente compatible. En efecto, de lo contrario, para ciertos $\Gamma \subseteq F'_n$, $\Delta \subseteq G'_n$, tendríamos $\vdash \{A_2\} \cup \Gamma \to \Delta$ y $\vdash \Gamma \to$ $\to \Delta \cup \{A_1\}$. Pero entonces $\vdash \{A_1 \supset A_2\} \cup \Gamma \to \Delta$, y el par F'_n, G'_n resultaría incompatible.

Si es compatible el par $\{A_2\} \cup F'_n, G'_n$, entonces tomamos $F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_2\rangle\}$, $G_{n+1} = Q_n$. Si es compatible el par $F'_n, G'_n \cup \{A_1\}$, entonces tomamos $F_{n+1} = P_n$, $G_{n+1} =$ $= Q_n \cup \{\langle 2h_n + 3, A_1\rangle\}$.

6) $\langle m, A\rangle \in G_n$, $A = A_1 \supset A_2$.

Entonces,

$$F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1\rangle\},$$
$$G_{n+1} = Q_n \cup \{\langle 2h_n + 5, A_2\rangle\}.$$

7) $\langle m, A\rangle \in F_n$, $A = \neg A_1$.

Entonces,

$$F_{n+1} = P_n, G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_1\rangle\}.$$

8) $\langle m, A\rangle \in G_n$, $A = \neg A_1$.
Entonces,

$$F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1\rangle\}, \quad G_{n+1} = Q_n.$$

9) $\langle m, A\rangle \in F_n$, $A = \forall\, x A_1(x)$.

Sean $t_1, \ldots, t_n$ los primeros n términos de la sucesión de todos los términos cerrados del lenguaje Ψ. Entonces,

$$F_{n+1} = P_n \cup \{\langle 2(h_n + j) + 1, A_1(t_j)\rangle \mid j = 1, \ldots, n\}, \quad G_{n+1} = Q_n.$$

10) $\langle m, A\rangle \in G_n$, $A = \forall\, x A_1(x)$.

Tomemos la primera constante $a \in V$ que no figura en $F'_n \cup G'_n$. Tomemos $F_{n+1} = P_n$, $G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_1(a)\rangle\}$. El par F'_{n+1}, G'_{n+1} es compatible. En caso contrario, para ciertos $\Gamma \subseteq F'_n$, $\Delta \subseteq G'_n$, tendríamos $\vdash \Gamma \to \Delta \cup \{A_1(a)\}$. Puesto que la constante a no figura en Γ y Δ, en la deducción $\vdash \Gamma \to \Delta \cup$ $\cup \{A_1(a)\}$ esta constante se puede sustituir por una nueva variable z que no figura en la deducción y obtener la deducción $\vdash \Gamma \to$ $\to \Delta \cup \{A_1(z)\}$; seguidamente, de acuerdo con las reglas del cálculo de predicados, se puede obtener $\vdash \Gamma \to \Delta \cup \{\forall\, x A_1(x)\}$, de donde, en virtud de $\forall\, x A_1(x) \in G'_n$, se deduce la incompatibilidad del par F'_n, G'_n.

11) $\langle m, A\rangle \in F_n$, $A = \exists\, x A_1(x)$.

Tomemos la primera constante $a \in V$ que no figura en $F'_n \cup G'_n$. Tomemos $F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1(a)\rangle\}$, $G_{n+1} = Q_n$. Vemos que el par F'_{n+1}, G'_{n+1} es compatible.

12) $\langle m, A\rangle \in G_n$, $A = \exists\, x A_1(x)$.

Sean $t_1, \ldots, t_n$ los primeros n términos de la sucesión de todos los términos cerrados del lenguaje Ψ. Entonces,

$$F_{n+1} = P_n, \quad G_{n+1} = Q_n \cup \{\langle 2(h_n + j) + 1, A_1(t_j)\rangle \mid j = 1, \ldots, n\}.$$

Finalmente, si para el elemento $\langle m, A\rangle$ no se cumple ninguno de los casos 1–12, entonces tomamos

$$F_{n+1} = P_n, \quad G_{n+1} = Q_n.$$

En este caso, en comparación con F_n y G_n sólo cambia el orden del elemento de turno, siendo $F'_{n+1} = F_n$, $G'_{n+1} = G'_n$.

Ahora queda tomar por definición

$$Y = \bigcup_{n\in\omega} F'_n, \quad Z = \bigcup_{n\in\omega} G'_n.$$

Cada par F'_n, G'_n era compatible, de donde se deduce la compatibilidad de Y, Z. No es difícil demostrar la completitud de Y, Z. Comprobemos, por ejemplo, el cumplimiento de la exigencia 6 de la definición de completitud.

Supongamos que $(A \supset B) \in Z$. Entonces, $\langle m, A \supset B\rangle \in G_n$ para ciertos m y n. Aumentando en caso de necesidad el número n, podemos lograr que el elemento $\langle m, A \supset B\rangle$ sea el elemento de turno en G_n. De acuerdo con el método de construcción, tenemos $A \in F'_{n+1}$, $B \in G'_{n+1}$, es decir, $A \in Y$ y $B \in Z$. El lema queda demostrado. ◄

Ahora podemos construir el modelo buscado M. Como objetos del modelo tomemos el conjunto de todas las expresiones de la forma $[t]$, donde t es un término cerrado arbitrario del lenguaje Ψ. A la constante c del lenguaje Ω le asignamos el objeto $[c]$ del modelo M. Al símbolo de función m-ádico f del lenguaje Ω le asignamos la función $\widetilde{f}$ en el modelo M. A saber, para objetos arbitrarios $[t_1], \ldots, [t_m]$ del modelo M definimos $\widetilde{f}([t_1], \ldots, [t_m]) = [f(t_1, \ldots, t_m)]$, donde en el segundo miembro entre corchetes se encuentra un término cerrado del lenguaje Ψ.

Finalmente, asignemos al símbolo de predicado m-ádico P del lenguaje Ω el predicado $\widetilde{P}$ del modelo M. A saber, $\widetilde{P}([t_1], \ldots, [t_m])$ es verdadero si y sólo si la fórmula $P(t_1, \ldots, t_m)$ pertenece al conjunto Y indicado en el lema.

La construcción de M ha concluido. Es necesario comprobar si las sentencias del conjunto X son verdaderas en M. Para esto, demostremos las dos afirmaciones siguientes, que establecen la relación de los conjuntos Y, Z con la veracidad en el modelo M. Supongamos que

A es una fórmula valorada en el modelo M, y

A^* es la sentencia del lenguaje Ψ que se obtiene si en A se eliminan todos los corchetes.

Entonces,

a) $A^* \in Y \Rightarrow M \models A$,

b) $A^* \in Z \Rightarrow$ es falso $M \models A$.

Demostraremos ambas afirmaciones simultáneamente, por inducción respecto a la construcción de la fórmula A.

Si A es una fórmula atómica y $A^* \in Y$, entonces $M \models A$, por definición de veracidad en M. Si $A^* \in Z$, entonces, en virtud de la compatibilidad de Y, Z, tenemos $A^* \notin Y$ y, por tanto, no $M \models A$.

Supongamos que $A = A_1 \wedge A_2$. Si $A^* \in Y$, entonces, en virtud de la completitud, $A_1^*, A_2^* \in Y$. Entonces, según la hipótesis de inducción, $M \models A_1, M \models A_2$, es decir, $M \models A_1 \wedge A_2$. Si $A^* \in Z$, entonces, nuevamente en virtud de la completitud, $A_1^* \in Z$ o $A_2^* \in Z$. Según la hipótesis de inducción, no $M \models A_1$ o $M \models A_2$, lo que significa no $M \models A_1 \wedge A_2$.

De manera análoga se consideran los demás casos de construcción de A. Consideremos el caso cuando $A = \exists x A_1(x)$.

Si $A^* \in Y$, entonces, en virtud de la completitud, $A_1^*(a) \in Y$ para cierta constante de V. Según la hipótesis de inducción, $M \models A_1([a])$, es decir, $M \models \exists x A_1(x)$. Si $A^* \in Z$, entonces, en virtud de la completitud, $A_1^*(t) \in Z$ para todo término cerrado t del lenguaje Ψ. Según la hipótesis de inducción, no $M \models A_1([t])$ para todo t y, por tanto, no $M \models \exists x A_1(x)$.

Ahora, puesto que $X \subseteq Y$, de la afirmación a) se deduce que $M \models A$ para toda $A \in X$ y, por tanto, M es un modelo de la teoría T. ◄

3.2.2 Señalemos algunas consecuencias del teorema fundamental de la subsección 3.2.1.

Teorema de compacidad de Máltsev. *Sea X un conjunto de sentencias del lenguaje Ω. Si todo subconjunto finito del conjunto X tiene un modelo, entonces todo el conjunto X también tiene un modelo.*

► En efecto, de acuerdo con las condiciones del teorema, X forma una teoría axiomática consistente, puesto que si en X se dedujera una contradicción, entonces existiría un conjunto finito $\Gamma \subseteq X$, $\Gamma \vdash C \wedge \neg C$, es decir, el conjunto finito Γ no tendría modelo. De acuerdo con el teorema fundamental, X tiene un modelo. ◄

Teorema de completitud del cálculo de predicados. *Si una fórmula A es una ley lógica, entonces A se deduce en el cálculo de predicados.*

► Se puede considerar que A es una sentencia (en caso de necesidad, A se puede cerrar con cuantificadores universales). Si A no se deduce en el cálculo de predicados, entonces

la teoría T con axioma no lógico único $\neg A$ es consistente (ya que de $\neg A \vdash C \wedge \neg C$ se deduciría $\vdash A$). De acuerdo con el teorema fundamental, $\neg A$ tiene un modelo M. Pero entonces es falso $M \models A$ y, por tanto, A no es una ley lógica. ◀

3.2.3 Añadamos al lenguaje Ar una nueva constante c, y a la teoría Ar un número infinito de axiomas no lógicos $0 < c$, $\widetilde{1} < c$, $\widetilde{2} < c, \ldots$. Aquí, $\widetilde{n}$ es un término de la forma $SS \ldots S0$, correspondiente al número natural n.

Toda subteoría finita de la teoría T tiene un modelo. En efecto, si en una subteoría finita figuran sólo los axiomas $\widetilde{n} < c$ con números n menores que j, entonces es suficiente tomar el modelo estándar ω y asignar a la constante c el número $(j+1)$.

Según el teorema de compacidad, la teoría T tiene un modelo. Este modelo, por supuesto, será también un modelo de Ar, pero éste será un *modelo no estándar*, no isomorfo a ω. En efecto, en este modelo, a la constante c le corresponde un objeto mayor que todos los objetos estándares, que corresponden a los números naturales habituales $0, 1, 2, \ldots$.

Señalemos que esto ocurre a pesar de que tiene lugar el conocido teorema sobre la categoricidad del conjunto de los números naturales. Este fenómeno ya fue discutido por nosotros en el capítulo dedicado a la teoría de conjuntos.

3.2.4 Si los símbolos de un lenguaje de primer orden Ω forman un conjunto finito o numerable, entonces el modelo M de la teoría consistente T que fue construido en el teorema fundamental es numerable. De aquí se deduce un resultado que es una variante del conocido teorema de Löwenheim—Skolem.

Teorema. *Sea Ω un lenguaje de primer orden con un conjunto numerable de símbolos. Si T es una teoría consistente en el lenguaje Ω, entonces la teoría T tiene un modelo con portador numerable.*

En particular, si Ω es un lenguaje de primer orden con un conjunto numerable de símbolos y M es un modelo arbitrario del lenguaje Ω, entonces existe también un modelo numerable M' tal que

$$\mathrm{Th}_\Omega(M) = \mathrm{Th}_\Omega(M').$$

Con $\mathrm{Th}_\Omega(M)$ se denota el conjunto de todas las sentencias del lenguaje Ω que son verdaderas en el modelo M.

En la terminología generalmente aceptada, esta observación puede ser formulada de la siguiente manera: *todo modelo de un lenguaje numerable es elementalmente equivalente a un modelo numerable.*

3.2.5 De los resultados obtenidos se deduce que si la teoría de conjuntos ZF es consistente, entonces ella tiene un modelo numerable. Esta afirmación es válida a pesar de que en ZF se puede demostrar la existencia de un conjunto no numerable. Ésta es la denominada *paradoja de Skolem*, ya discutida anteriormente (véase la subsección 1.6.5). Debemos subrayar nuevamente que este fenómeno no es una paradoja en el sentido propio de la palabra y no hay ninguna contradicción en el resultado obtenido.

la teoría T con axioma no lógico único $\neg A$ es consistente (ya que de $\neg A \vdash C \wedge \neg C$ se deduciría $\vdash A$). De acuerdo con el teorema fundamental, $\neg A$ tiene un modelo M. Pero entonces es falso $M \models A$ y, por tanto, A no es una ley lógica. ◀

3.2.3 Añadamos al lenguaje Ar una nueva constante c, y a la teoría Ar un número infinito de axiomas no lógicos $0 < c$, $\widetilde{1} < c$, $\widetilde{2} < c, \ldots$. Aquí, $\widetilde{n}$ es un término de la forma $SS \ldots S0$, correspondiente al número natural n.

Toda subteoría finita de la teoría T tiene un modelo. En efecto, si en una subteoría finita figuran sólo los axiomas $\widetilde{n} < c$ con números n menores que j, entonces es suficiente tomar el modelo estándar ω y asignar a la constante c el número $(j+1)$.

Según el teorema de compacidad, la teoría T tiene un modelo. Este modelo, por supuesto, será también un modelo de Ar, pero éste será un *modelo no estándar*, no isomorfo a ω. En efecto, en este modelo, a la constante c le corresponde un objeto mayor que todos los objetos estándares, que corresponden a los números naturales habituales $0, 1, 2, \ldots$.

Señalemos que esto ocurre a pesar de que tiene lugar el conocido teorema sobre la categoricidad del conjunto de los números naturales. Este fenómeno ya fue discutido por nosotros en el capítulo dedicado a la teoría de conjuntos.

3.2.4 Si los símbolos de un lenguaje de primer orden Ω forman un conjunto finito o numerable, entonces el modelo M de la teoría consistente T que fue construido en el teorema fundamental es numerable. De aquí se deduce un resultado que es una variante del conocido teorema de Löwenheim—Skolem.

Teorema. *Sea Ω un lenguaje de primer orden con un conjunto numerable de símbolos. Si T es una teoría consistente en el lenguaje Ω, entonces la teoría T tiene un modelo con portador numerable.*

En particular, si Ω es un lenguaje de primer orden con un conjunto numerable de símbolos y M es un modelo arbitrario del lenguaje Ω, entonces existe también un modelo numerable M' tal que

$$\mathrm{Th}_\Omega(M) = \mathrm{Th}_\Omega(M').$$

Con $\mathrm{Th}_\Omega(M)$ se denota el conjunto de todas las sentencias del lenguaje Ω que son verdaderas en el modelo M.

En la terminología generalmente aceptada, esta observación puede ser formulada de la siguiente manera: *todo modelo de un lenguaje numerable es elementalmente equivalente a un modelo numerable.*

3.2.5 De los resultados obtenidos se deduce que si la teoría de conjuntos ZF es consistente, entonces ella tiene un modelo numerable. Esta afirmación es válida a pesar de que en ZF se puede demostrar la existencia de un conjunto no numerable. Ésta es la denominada *paradoja de Skolem*, ya discutida anteriormente (véase la subsección 1.6.5). Debemos subrayar nuevamente que este fenómeno no es una paradoja en el sentido propio de la palabra y no hay ninguna contradicción en el resultado obtenido.

3.3 Teorema de eliminación del corte

3.3.1 El concepto de *deducibilidad* en el cálculo de predicados desempeña un papel clave en la teoría de la demostración. Por esta razón, en el cálculo de predicados es importante saber transformar las deducciones en una forma cómoda para detectar su deducibilidad. Esto es aún más importante en nuestros días, cuando el problema de búsqueda automática de deducciones en teorías axiomáticas mediante el empleo de computadoras tiene una importancia crucial. La mayoría de los métodos de búsqueda de deducciones en el cálculo de predicados está basada en el conocido teorema de G. Gentzen sobre la eliminación del corte, que fue obtenido en 1934. Aquí veremos una variante de este teorema.

Consideremos un lenguaje lógico-matemático Ω.

Llamaremos *colección de fórmulas* a todo conjunto finito de fórmulas del lenguaje Ω en el cual se admiten repeticiones de fórmulas. El orden de las fórmulas en una colección de fórmulas Γ no tiene importancia, pero para cada una se indica cuántos ejemplares ella tiene en Γ. Las operaciones con las colecciones de fórmulas se deben interpretar en correspondencia con esto.

Por ejemplo, en la unión de colecciones de fórmulas, $\Gamma \cup \Delta$, las cantidades de ejemplares de cada fórmula se suman. Para la unión $\Gamma \cup \Delta$, escribiremos brevemente $\Gamma\Delta$, de modo que $\Gamma\Delta$ y $\Delta\Gamma$ representan un mismo conjunto. La colección $A\Gamma$ se obtiene añadiendo a la colección Γ un ejemplar de la fórmula A.

Llamaremos *secuencia* a toda figura de la forma $\Gamma \to \Delta$, donde Γ y Δ son colecciones de fórmulas.

Formulemos ahora cierto cálculo en el que se deducirán secuencias. Los *axiomas* de este cálculo son secuencias arbitrarias de la forma

$$A\Gamma \to \Delta A,$$

donde A es una fórmula *atómica* arbitraria de Ω.

Las *reglas de inferencia* del cálculo de secuencias están construidas simétricamente e introducen las conectivas lógicas por la izquierda y por la derecha:

$$(\supset\to)\quad \frac{B\Gamma \to \Delta;\ \Gamma \to \Delta A}{(A \supset B)\Gamma \to \Delta};\qquad (\to\supset)\quad \frac{A\Gamma \to \Delta B}{\Gamma \to \Delta(A \supset B)};$$

$$(\wedge\to)\quad \frac{AB\Gamma \to \Delta}{(A \wedge B)\Gamma \to \Delta};\qquad (\to\wedge)\quad \frac{\Gamma \to \Delta A;\ \Gamma \to \Delta B}{\Gamma \to \Delta(A \wedge B)};$$

$$(\vee\to)\quad \frac{A\Gamma \to \Delta;\ B\Gamma \to \Delta}{(A \vee B)\Gamma \to \Delta};\qquad (\to\vee)\quad \frac{\Gamma \to \Delta AB}{\Gamma \to \Delta(A \vee B)};$$

$$(\neg\to)\quad \frac{\Gamma \to \Delta A}{\neg A\Gamma \to \Delta};\qquad (\to\neg)\quad \frac{A\Gamma \to \Delta}{\Gamma \to \Delta\neg A};$$

$$(\forall\to)\quad \frac{A(x \,||\, t)\forall x A\Gamma \to \Delta}{\forall x A\Gamma \to \Delta};\qquad (\to\forall)\quad \frac{\Gamma \to \Delta(A(y \,||\, x))}{\Gamma \to \Delta\forall y A};$$

$$(\exists\to)\quad \frac{A(y \,||\, x)\Gamma \to \Delta}{\exists y A\Gamma \to \Delta};\qquad (\to\exists)\quad \frac{\Gamma \to \Delta\exists x A(A(x \,||\, t)}{\Gamma \to \Delta\exists x A}.$$

En las reglas ($\rightarrow \forall$) y ($\exists \rightarrow$), la variable x no aparece libre en la secuencia inferior de la regla de inferencia.

Las deducciones en el cálculo de secuencias se escribirán en forma de árboles, de la misma manera que las deducciones en el cálculo de predicados (véase la introducción del presente libro). La altura de la deducción será, como antes, el número de secuencias en la rama más larga de la deducción. Además, no diferenciaremos las fórmulas y las secuencias que se diferencian sólo en los nombres de las variables ligadas. De esta manera, si se tiene una deducción con secuencia inferior S, entonces esta misma deducción automáticamente se considerará una deducción para cualquier secuencia que se obtiene de S mediante el renombramiento de las variables ligadas.

Escribiremos $\vdash \Gamma \rightarrow \Delta$ si la secuencia $\Gamma \rightarrow \Delta$ es deducible en el cálculo de secuencias.

Las deducciones en el cálculo de secuencias tienen una particularidad: las secuencias superiores a una regla de inferencia están formadas sólo por subfórmulas de las fórmulas de la secuencia que se encuentra en la conclusión de la regla de inferencia. Brevemente, cuando las reglas de inferencia se analizan «de abajo hacia arriba», las fórmulas de las secuencias sólo se «fragmentan», no aparece ninguna fórmula extraña. En esto consiste precisamente la denominada *propiedad de subfórmula* del cálculo de secuencias. En muchos casos, esto facilita considerablemente la búsqueda de la deducción de una secuencia dada.

El resultado fundamental de esta sección consiste en que el cálculo de secuencias que hemos descrito es equivalente al cálculo de predicados habitual. De esta manera, la búsqueda de una deducción en el cálculo de predicados es equivalente a

la búsqueda de una deducción en el cálculo de secuencias. Para demostrar el resultado fundamental tendremos que investigar detalladamente el cálculo de secuencias. El resultado clave aquí es el teorema de eliminación del corte. Se denomina *corte* a la siguiente regla de inferencia:

$$\frac{\Gamma \to \Delta A;\ A\Gamma \to \Delta}{\Gamma \to \Delta}.$$

El teorema afirma que esta regla es admisible en el cálculo de secuencias, es decir, si en el cálculo de secuencias son deducibles las premisas $\Gamma \to \Delta A$ y $A\Gamma \to \Delta$ de esta regla, entonces necesariamente es deducible la secuencia $\Gamma \to \Delta$, la conclusión de la regla determinada. Supongamos que en una deducción se utiliza el corte junto con otras reglas. El teorema afirma que todos los cortes se pueden eliminar y obtener una deducción sin cortes.

Señalemos que la variante del cálculo de secuencias que analizamos aquí se diferencia de la que utilizaba Gentzen (véase [19]).

3.3.2 **Lema.** *Para toda fórmula A del lenguaje Ω, tenemos*

$$\vdash A\Gamma \to \Delta A \quad \textit{(sin corte)}.$$

► Efectuaremos la demostración por inducción respecto a la cantidad de símbolos lógicos en la fórmula A. Si A es una fórmula atómica, entonces la secuencia es simplemente un axioma. Consideremos sólo algunos de los casos de la inducción; los restantes se proponen al lector a manera de ejercicios.

Supongamos que $A = B \wedge C$. Según la hipótesis de inducción, $\vdash BC\Gamma \to \Delta B$ y $\vdash BC\Gamma \to \Delta C$. Entonces, de acuerdo con

la regla $(\to \wedge)$, tenemos $\vdash BC\Gamma \to \Delta(B \wedge C)$ y, seguidamente, de acuerdo con la regla $(\wedge \to)$, $\vdash (B \wedge C)\Gamma \to \Delta(B \wedge C)$.

Supongamos que $A = \forall x B(x)$. Sea z una variable que no aparece libre en la secuencia $\forall x B(x)\Gamma \to \Delta \forall x B(x)$. De acuerdo con la hipótesis de inducción, $\vdash B(z) \forall x B(x)\Gamma \to \Delta B(z)$. Según la regla $(\forall \to)$, de aquí obtenemos $\vdash \forall x B(x)\Gamma \to \Delta B(z)$ y, a continuación, de acuerdo con la regla $(\to \forall)$, obtenemos finalmente $\vdash \forall x B(x)\Gamma \to \Delta \forall x B(x)$. ◄

Si S es una secuencia, entonces mediante $S(x \parallel t)$ denotamos el resultado de la sustitución correcta del término t en lugar de las apariciones libres de la variable x en cada fórmula que es elemento de la secuencia S.

3.3.3 Lema. *Si $\vdash S$, z es una variable y t es un término, entonces $\vdash S(z \parallel t)$; en este caso, la deducción de la secuencia resultante tiene la misma altura y el mismo número de secuencias que la deducción inicial.*

► La demostración se efectuará por inducción respecto a la construcción de la deducción $\vdash S$. Si S es un axioma, entonces $S(z \parallel t)$ es también un axioma.

Debemos considerar todos los casos en los que S se obtiene según una de las reglas de inferencia. Consideremos como ejemplo sólo el caso cuando S se obtiene según la regla $(\to \forall)$. Entonces S tiene la forma $\Gamma \to \Delta \forall y A$ y se obtiene de una secuencia de la forma $\Gamma \to \Delta A(y \parallel x)$, donde la variable x no aparece libre en S.

Tomemos una variable u diferente de todas las variables que figuran en las fórmulas y términos considerados. Según la hi-

pótesis de inducción, de la deducibilidad de $\Gamma \to \Delta A(y \parallel x)$ se deduce la deducibilidad de la secuencia $\Gamma \to \Delta(A(y \parallel x)(x \parallel u))$, es decir, de la secuencia $\Gamma \to \Delta A(y \parallel u)$. Utilizando nuevamente la hipótesis de inducción, obtenemos que la secuencia $\Gamma(z \parallel t) \to$ $\to \Delta(z \parallel t)A(y \parallel u)(z \parallel t)$ es deducible. Aplicando luego la regla $(\to \forall)$, resulta $\vdash \Gamma(z \parallel t) \to \Delta(z \parallel t) \forall u A(y \parallel u)(z \parallel t)$. La fórmula $\forall u(A(y \parallel u)(z \parallel t))$ coincide con $(\forall y A)(z \parallel t)$ a excepción de un renombramiento de las variables ligadas. De esta manera, la deducción obtenida nos da la posibilidad de deducir la secuencia

$$\Gamma(z \parallel t) \to \Delta(z \parallel t)(\forall y A)(z \parallel t). \qquad \blacktriangleleft$$

3.3.4 Lema. *En el cálculo de secuencias son admisibles las siguientes reglas de debilitación:*

$$\frac{\Gamma \to \Delta}{A\Gamma \to \Delta}; \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta A}.$$

La admisibilidad significa que de la deducibilidad de la secuencia $\Gamma \to \Delta$ *se deduce que las secuencias* $A\Gamma \to \Delta$ *y* $\Gamma \to \Delta A$ *son también deducibles. Más aún, se puede afirmar en este caso que las deducciones resultantes tienen una altura no mayor y no contienen más secuencias que la deducción inicial.*

► Efectuemos la demostración por inducción respecto a la altura de la deducción dada, $\vdash \Gamma \to \Delta$. Si $\Gamma \to \Delta$ es un axioma, entonces también lo son las secuencias $A\Gamma \to \Delta$ y $\Gamma \to \Delta A$. Debemos analizar todos los casos en los que $\Gamma \to \Delta$ se obtiene de acuerdo con una de las reglas de inferencia. Supongamos, por ejemplo, que $\Gamma \to \Delta$ se obtiene de acuerdo con la regla $(\exists \to)$. En este caso, $\Gamma \to \Delta$ tiene la forma $\exists y B\Gamma' \to \Delta$

y se obtiene de una secuencia de la forma $B(y \parallel x)\Gamma' \to \Delta$. Tomemos una nueva variable u que no figure en las secuencias consideradas. Según el lema de la subsección 3.3.3, tenemos $\vdash B(y \parallel x)(x \parallel u)\Gamma' \to \Delta$, es decir, $\vdash B(y \parallel u)\Gamma' \to \Delta$; la altura y el número de secuencias en la deducción obtenida no varían. Según la hipótesis de inducción, $\vdash B(y \parallel \parallel u)A\Gamma' \to \Delta$ y $\vdash B(y \parallel u)\Gamma' \to \Delta A$. De aquí, según la regla $(\exists \to)$, deducimos $\exists u(B(y \parallel u))A\Gamma' \to \Delta$, $\exists u(B(y \parallel u))\Gamma' \to \to \Delta A$, lo que coincide con las secuencias buscadas a excepción de un renombramiento de las variables ligadas. En este razonamiento fue necesario cambiar el nombre de la variable x por el de la nueva variable u para que, después de añadir la fórmula A, se cumplieran las restricciones impuestas a las variables en la aplicación de la regla $(\exists \to)$. ◀

3.3.5 Lema. *En el cálculo de secuencias, todas las reglas de inferencia son invertibles. Esto significa que si la conclusión de una regla de inferencia del cálculo de secuencias es deducible, entonces son deducibles también sus (dos) premisas. En este caso también se puede afirmar que las deducciones resultantes tienen altura no mayor y no contienen más secuencias que la deducción inicial.*

▶ Para las reglas $(\forall \to)$ y $(\to \exists)$, la afirmación del lema se deduce directamente de la admisibilidad de la regla de debilitación (véase la subsección 3.3.4). Para cada una de las restantes reglas de inferencia, demostraremos por separado el lema por inducción respecto a la altura de la deducción de la conclusión.

Consideremos, por ejemplo, la regla $(\supset\to)$. Supongamos que $\vdash (A \supset B)\Gamma \to \Delta$. Demostremos que $\vdash B\Gamma \to \Delta$ y $\vdash \Gamma \to \Delta A$

por inducción respecto a la altura de la deducción dada. Si la deducción inicial es un axioma, entonces ambas secuencias resultantes son también axiomas (aquí es importante que la fórmula $A \supset B$ no es atómica, mientras que las fórmulas que figuran explícitamente en la formulación de los axiomas sí lo son). A continuación se debe considerar el caso cuando la secuencia $(A \supset B)\Gamma \to \Delta$ se obtiene según una de las reglas de inferencia. Aquí tenemos dos casos:

a) la regla indicada no afecta la fórmula escrita explícitamente, $A \supset B$;

b) la regla indicada afecta esta fórmula.

En el caso *a*, los razonamientos son de un mismo tipo para todas las reglas. Supongamos, por ejemplo, que $(A \supset B)\Gamma \to \Delta$ se obtiene según la regla $(\to \forall)$. Entonces esta secuencia tiene la forma $(A \supset B)\Gamma \to \Delta' \forall y C$ y se obtiene de la secuencia $(A \supset \supset B)\Gamma \to \Delta' C(y \parallel x)$. De acuerdo con la hipótesis de inducción, las secuencias $B\Gamma \to \Delta'(C(y \parallel x))$ y $\Gamma \to \Delta' A(C(y \parallel x))$ son deducibles. Aplicando a ellas la regla $(\to \forall)$, obtenemos las secuencias buscadas.

En el caso *b*, la afirmación es trivial. Las secuencias buscadas son premisas de la regla de inferencia $(\supset\to)$ y, por consiguiente, son deducibles. ◀

3.3.6 **Lema.** *En el cálculo de secuencias, son admisibles las reglas de contracción:*

$$\frac{AA\Gamma \to \Delta}{A\Gamma \to \Delta}; \quad \frac{\Gamma \to \Delta AA}{\Gamma \to \Delta A},$$

es decir, de la deducibilidad de las premisas de estas reglas se deduce la deducibilidad de las conclusiones. En este caso también

se puede afirmar que la deducción de las conclusiones tiene altura no mayor y no contienen más secuencias que la deducción de las premisas correspondientes.

► Demostremos para todo número natural n la siguiente afirmación: si en una deducción de una secuencia S, o bien a la izquierda, o bien a la derecha, en S se repite cierta fórmula A (es decir, S tiene una de las formas $AA\Gamma \to \Delta$ o $\Gamma \to \Delta AA$), y la altura de la deducción dada no excede n, entonces también es deducible la secuencia S', que se obtiene mediante la sustitución de los dos ejemplares señalados de la fórmula A por un ejemplar (es decir, S' tiene una de las formas $A\Gamma \to \Delta$ o $\Gamma \to \Delta A$, respectivamente). En este caso, la deducción S' tiene altura no mayor y no contiene más secuencias que la deducción dada de S.

Demostremos esta afirmación por inducción respecto a n. Para $n = 1$, la secuencia S es un axioma. Pero entonces, evidentemente, S' es también un axioma.

Se deben analizar todos los casos cuando la secuencia S se obtiene según una de las reglas de inferencia. Aquí se tienen dos casos:

a) la regla según la cual se obtiene S no afecta ninguno de los ejemplares considerados de la fórmula que se contrae, A;

b) la regla según la cual se obtiene S afecta uno de los ejemplares de la fórmula que se contrae, A.

En el caso *a*, los razonamientos son de un mismo tipo para todas las reglas. Supongamos, por ejemplo, que S tiene la forma $AA\Gamma \to \Delta'(C \supset D)$ y se obtiene de la secuencia $AAC\Gamma \to \Delta' D$ según la regla $(\to\supset)$. De la deducibilidad de esta secuencia y

de la hipótesis de inducción, se obtiene la deducibilidad de la secuencia $AC\Gamma \to \Delta' D$. Luego, aplicando a esta secuencia la regla $(\to\supset)$, obtenemos la deducción de la secuencia S'.

En el caso *b*, es esencial que las reglas de inferencia son invertibles. Supongamos, por ejemplo, que A tiene la forma $(C \supset D)$ y que la secuencia S tiene la forma $(C \supset D)(C \supset D)$ $\Gamma \to \Delta$ y se obtiene de las dos secuencias $D(C \supset D)\Gamma \to \Delta$ y $(C \supset D)\Gamma \to \Delta C$ según la regla de inferencia $(\supset\to)$. Puesto que la regla $(\supset\to)$ es invertible, de la deducibilidad de las dos últimas secuencias concluimos que también son deducibles las secuencias $DD\Gamma \to \Delta$ y $\Gamma \to \Delta CC$, con ayuda de deducciones cuya complejidad no es mayor que la de las deducciones correspondientes de las secuencias anteriores. Según la hipótesis de inducción, de aquí llegamos a la conclusión de que también son deducibles las secuencias $D\Gamma \to \Delta$ y $\Gamma \to \Delta C$. Según la regla $(\supset\to)$, de aquí obtenemos la deducción de

$$(C \supset D)\Gamma \to \Delta.$$

Consideremos además el caso cuando la secuencia S tiene la forma $\Gamma \to \Delta \exists\, yB(y)\, \exists\, yB(y)$ y se obtiene de la secuencia

$$\Gamma \to \Delta B(t)\, \exists\, yB(y)\, \exists\, yB(y)$$

según la regla de inferencia $(\to \exists)$. Según la hipótesis de inducción, $\vdash \Gamma \to \Delta B(t)\, \exists\, yB(y)$ y es suficiente aplicar a esta última secuencia la regla $(\to \exists)$ para obtener la deducción de S'. ◄

3.3.7 Teorema de Gentzen. *En el cálculo de secuencias, es admisible el corte:*

$$\frac{\Gamma \to \Delta A;\ A\Gamma \to \Delta}{\Gamma \to \Delta}.$$

► Demostraremos la afirmación por inducción respecto a la cantidad de símbolos lógicos de la fórmula A. Demostraremos esta afirmación por inducción respecto a la suma de las alturas de las deducciones dadas de $\Gamma \to \Delta A$ y $A\Gamma \to \Delta$ para una complejidad fija de A.

La base de esta inducción doble consiste en el análisis del caso cuando A es una fórmula atómica y ambas secuencias deducibles son axiomas. Nosotros afirmamos que en este caso $\Gamma \to \Delta$ es también un axioma. En efecto, si $A \in \Gamma$ y $A \in \Delta$, entonces la afirmación es evidente. Supongamos, por ejemplo, que $A \notin \Gamma$. En virtud de que $\Gamma \to \Delta A$ es un axioma, existe una fórmula atómica B tal que $B \in \Gamma$ y $B \in \Delta$. Pero entonces $\Gamma \to \Delta$ es un axioma.

Analicemos ahora algunos de los casos de la inducción.

Supongamos que A tiene la forma $(C \supset D)$ y tenemos $\vdash \Gamma \to \Delta(C \supset D)$ y $\vdash (C \supset D)\Gamma \to \Delta$. En virtud de que las reglas $(\to\supset)$ y $(\supset\to)$ son invertibles, las secuencias $C\Gamma \to \Delta$, $D\Gamma \to \Delta$ y $\Gamma \to \Delta C$ son deducibles. Aplicando a $D\Gamma \to \Delta$ la regla de debilitación, obtenemos $\vdash DC\Gamma \to \Delta$. De $\vdash C\Gamma \to \Delta D$ y $\vdash DC\Gamma \to \Delta$, según la regla del corte (esta regla puede ser aplicada en virtud de la inducción respecto a la complejidad de la fórmula), obtenemos $\vdash C\Gamma \to \Delta$. A continuación, aplicamos la regla del corte con secuencia $\vdash \Gamma \to \Delta C$ y obtenemos $\vdash \Gamma \to \Delta$.

Supongamos que A tiene la forma $\exists\, xB(x)$ y tenemos $\vdash \Gamma \to \Delta\exists\, xB(x)$ y $\vdash \exists\, xB(x)\Gamma \to \Delta$. Si $\Gamma \to \Delta\exists\, xB(x)$ es un axioma, entonces $\Gamma \to \Delta$ es también un axioma y, por tanto, $\vdash \Gamma \to \Delta$ (aquí tenemos en cuenta que $\exists\, xB(x)$ no es una fórmula atómica). Supongamos que $\Gamma \to \Delta\exists\, xB(x)$ se obtiene según una de las reglas de inferencia. Aquí tenemos dos casos:

a) esta regla de inferencia no afecta la aparición considerada de $\exists\, xB(x)$;

b) esta regla de inferencia es $(\to \exists)$, la cual afecta la aparición considerada de $\exists\, xB(x)$.

En el caso *a*, los razonamientos son de un mismo tipo para todas las reglas. Supongamos, por ejemplo, que $\Gamma \to \to \Delta\exists\, xB(x)$ tiene la forma $\Gamma \to \Delta'\neg D\exists\, xB(x)$ y se obtiene de $D\Gamma \to \Delta'\exists\, xB(x)$ según la regla $(\to \neg)$. De la deducción dada $\vdash \exists\, xB(x)\Gamma \to \Delta'\neg D$, en virtud de que la regla $(\to \neg)$ es invertible, concluimos que $\vdash \exists\, xB(x)D\Gamma \to \Delta'$, y la altura de esta última deducción no excede la altura de la deducción de la secuencia $\exists\, xB(x)\Gamma \to \Delta'\neg D$. Según la hipótesis de inducción (inducción respecto a la suma de las alturas de las deducciones), aplicamos el corte a $D\Gamma \to \Delta'\exists\, xB(x)$ y $\exists\, xB(x)D\Gamma \to \Delta'$; obtenemos como resultado $\vdash D\Gamma \to \Delta'$. A continuación, aplicamos $(\to \neg)$, y obtenemos $\vdash \Gamma \to \Delta$.

En el caso *b*, la secuencia $\Gamma \to \Delta\exists\, xB(x)$ se obtiene de la secuencia $\Gamma \to \Delta B(t)\exists\, xB(x)$ según la regla $(\to \exists)$. De la deducción dada $\vdash \exists\, xB(x)\Gamma \to \Delta$, según la regla de debilitación, obtenemos $\vdash \exists\, xB(x)\Gamma \to \Delta B(t)$, y la altura de la deducción resultante no es mayor. Según la hipótesis de inducción (inducción respecto a la suma de las alturas de las deducciones), aplicamos el corte a

$$\Gamma \to \Delta B(t)\exists\, xB(x) \quad \text{y} \quad \exists\, xB(x)\Gamma \to \Delta B(t),$$

y obtenemos $\vdash \Gamma \to \Delta B(t)$.

A continuación, de $\vdash \exists\, xB(x)\Gamma \to \Delta$, en virtud de que la regla $(\exists \to)$ es invertible, obtenemos $\vdash B(y)\Gamma \to \Delta$ con la nueva variable y. Luego, de acuerdo con el lema de sustitución (véase

la subsección 3.3.3), de aquí obtenemos $\vdash B(t)\Gamma \to \Delta$. Según la hipótesis de inducción (inducción respecto a la complejidad de la fórmula), se puede aplicar el corte a $\Gamma \to \Delta B(t)$ y $B(t)\Gamma \to \Delta$ y, de esta manera, obtener $\vdash \Gamma \to \Delta$. ◀

3.3.8 Ahora estamos en condiciones de establecer la equivalencia del cálculo de predicados y el cálculo de secuencias. Esta equivalencia se formula en los dos lemas siguientes.

Lema. *Si en el cálculo de predicados la fórmula A es deducible, entonces en el cálculo de secuencias la secuencia $\to A$ es deducible.*

► Efectuaremos la demostración por inducción respecto a la construcción de la deducción $\vdash A$ en el cálculo de predicados. Primeramente, se deben deducir en el cálculo de secuencias todos los axiomas del cálculo de predicados. Éste es un ejercicio simple de deducibilidad en el cálculo de secuencias. Consideremos sólo dos ejemplos.

Demostremos $\vdash\to (A \supset C) \supset . (B \supset C) \supset (A \vee B \supset C)$. En efecto, según el lema de la subsección 3.3.2, $\vdash (A \supset C), (B \supset C) \to (A \supset C)$. En virtud de que la regla $(\to\supset)$ es invertible, obtenemos

$$\vdash A \supset C, \quad B \supset C, \quad A \to C.$$

Análogamente, obtenemos

$$\vdash A \supset C, \quad B \supset C, \quad B \to C.$$

De estas dos secuencias, en virtud de la regla $(\vee \to)$, deducimos

$$\vdash A \supset C, \quad B \supset C, \quad A \vee B \to C.$$

Aplicando varias veces la regla $(\to\supset)$, deducimos la secuencia exigida.

Demostremos $\vdash\!\!\rightarrow \forall x(C \supset A(x)) \supset . C \supset \forall x A(x)$, donde C no contiene apariciones libres de x. Según el lema de la subsección 3.3.2,

$$\vdash \forall x(C \supset A(x)), \quad C \supset A(x) \rightarrow C \supset A(x).$$

Según la regla $(\forall \rightarrow)$, de aquí obtenemos

$$\vdash \forall x(C \supset A(x)) \rightarrow C \supset A(x).$$

En virtud de que la regla $(\rightarrow\supset)$ es invertible, resulta

$$\vdash \forall x(C \supset A(x)), \quad C \rightarrow A(x).$$

Aplicando la regla $(\rightarrow \forall)$, obtenemos

$$\vdash \forall x(C \supset A(x)), \quad C \rightarrow \forall x A(x)$$

Nótese que las exigencias impuestas sobre las variables en esta regla se cumplen precisamente gracias a que C no contiene apariciones libres de x. Aplicando a la última secuencia varias veces la regla $(\rightarrow\supset)$, obtenemos la deducibilidad de la secuencia necesaria.

Luego, es necesario comprobar si las reglas de inferencia del cálculo de predicados conservan la deducibilidad en el cálculo de secuencias. Supongamos, por ejemplo, que $\vdash\!\!\rightarrow A$ y $\vdash\!\!\rightarrow (A \supset B)$. Demostremos que en este caso $\vdash\!\!\rightarrow B$.

En virtud de que la regla $(\rightarrow\supset)$ es invertible, de $\vdash\!\!\rightarrow (A \supset B)$ se deduce $\vdash A \rightarrow B$. De $\vdash\!\!\rightarrow A$, según la regla de debilitación, obtenemos $\vdash\!\!\rightarrow B, A$. Ahora queda aplicar el corte a las secuencias deducibles $\rightarrow B, A$ y $A \rightarrow B$, como resultado de lo cual obtenemos la secuencia $\rightarrow B$. ◄

Definamos para cada secuencia $\Gamma \to \Delta$ cierta fórmula $(\Gamma \to \to \Delta)^0$, que es la traducción de la secuencia dada a una fórmula del cálculo de predicados. A saber, la traducción de $A_1, \ldots, A_n \to \to B_1, \ldots, B_m$ es, por definición, la fórmula $A_1 \wedge \ldots \wedge A_n \supset \supset B_1 \vee \ldots \vee B_m$. La traducción de la secuencia $\to B_1, \ldots, B_m$ es la fórmula $B_1 \vee \ldots \vee B_m$. La traducción de la secuencia $A_1, \ldots, A_n \to$ es la fórmula $\neg(A_1 \wedge \ldots \wedge A_n)$. Finalmente, la traducción de la secuencia $\to$ es la fórmula $A \wedge \neg A$ para cierta fórmula fija A.

Lema. *Si una secuencia S es deducible en el cálculo de secuencias, entonces la fórmula S^0 es deducible en el cálculo de predicados.*

► Es necesario verificar si la traducción de todo axioma del cálculo de secuencias es deducible en el cálculo de predicados, y que la traducción de toda regla de inferencia es admisible en el cálculo de predicados. Todos estas afirmaciones se pueden demostrar con ayuda de la técnica de deducción natural en el cálculo de predicados (véase [11]), pero también se puede aplicar el teorema de completitud del cálculo de predicados y verificar que si las traducciones de las premisas de una regla de inferencia del cálculo de secuencias son leyes lógicas, entonces también la conclusión es una ley lógica. ◄

3.4

Sobre el programa de Hilbert de fundamentación de la matemática

3.4.1 El ejemplo de la teoría ingenua de conjuntos demuestra que una teoría matemática de interés general puede resultar internamente contradictoria. Los motivos de esto se pueden buscar en la peculiaridad de

a) los objetos de investigación en la matemática,

b) los métodos de razonamiento aplicados a estos objetos.

En la matemática los objetos de la investigación no son, por lo general, experimentalmente observables. Estos objetos son imaginarios, y constituyen el resultado de complejas abstracciones sucesivas. En efecto, ¿en qué sentido concreto existen los números irracionales, los conjuntos no medibles de números reales, la función de Dirichlet, el conjunto perfecto nunca denso de Cantor, etcétera?

El método de razonamiento que se aplica a estos complicados objetos también se obtiene mediante una compleja extrapolación de los métodos de razonamiento que se utilizan en la vida cotidiana o, al menos, en el ámbito científico habitual.

Sin embargo, los métodos de razonamiento aplicados de este modo a los objetos ideales pueden conducir a consecuencias inesperadas. Por ejemplo, el matemático tiende, por lo visto, a pensar que el conjunto de puntos

$$\{\langle x, y, z\rangle \mid \sqrt{x^2 + y^2 + z^2} \leqslant 1\}$$

del espacio euclídeo tridimensional puede servir como un buen modelo de un cuerpo geométrico, a saber, de una bola del espacio tridimensional. No obstante, en ZFC se puede demostrar que esta «bola» puede ser dividida en cuatro subconjuntos de los cuales con ayuda de movimientos en el espacio euclídeo se pueden formar dos bolas iguales a la inicial.

Consecuencias de este tipo despiertan sospechas de que una serie de resultados obtenidos en el marco de una teoría matemática determinada, incluso consistente, no tiene sencillamente ninguna relación con la realidad física y es resultado de una extrapolación que ha ido demasiado lejos. Esto, a su vez, suscita una serie de complicadas cuestiones filosóficas relacionadas con el valor y la rigurosidad del razonamiento matemático, con la correspondencia entre los resultados matemáticos demostrados y las leyes del mundo circundante.

Asimismo, puede provocar inquietud la incompletitud de las teorías matemáticas. Como ya hemos señalado, se ha demostrado que muchas afirmaciones interesantes de la teoría de conjuntos (por ejemplo, la hipótesis del continuo) no pue-

den ser deducidas ni refutadas en el sistema ZFC. Sin embargo, no se ve ningún principio intuitivamente evidente que se debería añadir a ZFC para resolver la cuestión sobre la veracidad de dichas afirmaciones. Al contrario, los experimentos muestran que se pueden proponer sistemas axiomáticos de tanto contenido, matemáticamente tan interesantes, que amplían ZFC y en los cuales el problema sobre la veracidad de las afirmaciones mencionadas se resuelve de diferentes maneras. Esto nuevamente nos convence de que es erróneo en esencia plantear la pregunta de si la hipótesis del continuo es «en realidad» verdadera. ¿Qué significa «en realidad»? No existe ningún «en realidad». La hipótesis del continuo es una afirmación sobre objetos imaginarios, y la cuestión sobre su veracidad depende esencialmente de los métodos de razonamiento aplicados a estos objetos.

Gödel demostró que toda teoría axiomática formal suficientemente rica y efectivamente axiomatizada es necesariamente incompleta. Así pues, es imposible describir efectivamente en forma de teoría axiomática formal incluso un campo relativamente tan estrecho de la matemática como la teoría de los números naturales. Más aún, al intentar efectuar esta descripción aparecen enunciados que son independientes de la teoría construida, es decir, tales que se puede obtener una teoría sin contradicciones tanto si se agrega el enunciado en cuestión como si se agrega su negación. De acuerdo con el teorema de existencia de un modelo (véase la sección 3.2), en este caso tanto la teoría con dicho enunciado como la teoría con la negación de éste tienen modelos, lo que nuevamente puede tomarse como un argumento en favor de la inexistencia de una teoría «absolutamente verdadera, la única correcta».

Finalmente, el método clásico de razonamiento conduce a menudo a que se demuestra la existencia de los objetos, pero no se indica ningún método de construcción de los mismos, incluso si se trata de objetos de naturaleza simple, que, en principio, se podrían definir efectivamente. Por ejemplo, se demuestra que toda función continua en un intervalo alcanza su máximo en cierto punto; sin embargo, esta demostración no ofrece ningún método para hallar este punto. A menudo, en favor de este teorema citan los dos argumentos siguientes: en primer lugar, este teorema parece geométricamente evidente; en segundo lugar, hasta ahora nadie ha logrado proponer un ejemplo de función continua que no tenga máximo en un intervalo y refutar con ello el teorema. En lo que se refiere al primer argumento, se puede responder que él está completamente fuera del asunto. La afirmación del teorema puede ser geométricamente evidente, pero aquí no se trata de geometría intuitiva, sino de cierto modelo teórico-conjuntista exacto de continuidad, y la cuestión consiste en si este modelo corresponde suficientemente o no a la intuición. La ingeniosa demostración teórico-conjuntista presentada en este caso está llamada precisamente a convencernos de que el modelo ha sido elegido adecuadamente. Pero ahora nosotros estamos impugnando precisamente esta demostración y no la evidencia intuitiva del hecho. En lo que se refiere al segundo argumento, incluso sin este teorema sabemos que algunas funciones continuas tienen máximo. Todo el significado del teorema consiste en que para toda función continua existe un punto donde se alcanza el máximo. Pero ¿qué significa la palabra «existe» en este teorema y cuál es el valor de la demostración de la existencia de un objeto cuando no se da ningún método para su construcción?

3.4.2 Vemos que tanto el objeto de investigación como el método de razonamiento de la matemática tradicional y, ante todo, de la matemática teórico-conjuntista dan lugar a una severa crítica.

El uso ilimitado de concepciones teórico-conjuntistas conduce a paradojas.

No se comprende en qué medida el objeto de investigación en la matemática corresponde a la realidad.

El método de razonamiento en la matemática conduce a demostraciones de existencia que no son efectivas, incluso en el caso de objetos simples.

Las causas de las paradojas se pueden atribuir a los métodos de formación de los conceptos, por ejemplo, al uso del axioma de abstracción ilimitada.

Para evitar paradojas, es suficiente utilizar la teoría limitada de conjuntos, por ejemplo, en el marco del sistema de Zermelo—Fraenkel. Sin embargo, es más difícil superar las demás objeciones. Aparte de todo esto, aún no está claro si el sistema de Zermelo—Fraenkel es consistente o no. Por ahora sólo contamos con observaciones pragmáticas que muestran que las paradojas conocidas no se deducen de modo habitual en este sistema.

La inefectividad en la matemática está relacionada con el hecho de que los métodos de razonamiento que se aplican a los conjuntos finitos fueron extrapolados a los conjuntos infinitos. En efecto, supongamos, por ejemplo, que $P(x)$ es un predicado donde x se considera como una variable que varía en el conjunto de los números naturales. La afirmación $\exists\, xP(x) \vee \neg\exists\, xP(x)$ se considera incondicionalmente válida (éste es un caso particular de la ley del tercero excluido), pero ¿cómo saber qué es válido precisamente: $\exists\, xP(x)$ o $\neg\exists\, xP(x)$? Podemos analizar sucesiva-

mente los números naturales $0, 1, 2, \ldots$ y convencernos sucesivamente de que $\neg P(0), \neg P(1), \ldots$, pero debido a que el conjunto de los números naturales es infinito es imposible de esta manera demostrar que $\neg \exists\, x P(x)$. La única esperanza puede ser encontrar un número natural n para el cual $P(n)$.

Señalemos también que las concepciones físicas modernas no ofrecen razones para suponer que en la naturaleza existen conjuntos actualmente infinitos. La matemática muy a menudo opera con conjuntos infinitos como ω, $P(\omega)$, etcétera, considerándolos objetos de investigación acabados y realmente definidos. En esto consiste el uso de la *abstracción del infinito actual* en la matemática. Muchos matemáticos, a partir de Gauss, se han manifestado en contra de la aplicación de esta abstracción. No obstante, los conjuntos actualmente infinitos se utilizan ampliamente y tienen gran importancia en la matemática moderna.

Con mayor cuidado se aplica en la matemática la *abstracción de realizabilidad potencial*, cuando se admite sólo la posibilidad de continuar ilimitadamente las construcciones en cuestión y se ignoran las dificultades técnicas temporales, pero no se considera que existe el conjunto de todos los resultados de estas construcciones. Las abstracciones de este tipo son absolutamente suficientes, por ejemplo, para la construcción de la mayor parte de la teoría de los números naturales.

3.4.3 Hilbert, en una serie de trabajos publicados entre los años 1926 y 1928, propuso un método radical para resolver las dificultades discutidas anteriormente.

Él propuso dividir las sentencias de la matemática clásica en *reales* e *ideales*. Se considera que sólo las sentencias reales tienen

sentido informal. Las sentencias reales deben referirse sólo a objetos constructivos simples, ellas no pueden utilizar el infinito actual. La comprensión de los casos en que una sentencia real es verdadera no debe provocar objeciones desde el punto de vista de la crítica anterior. En cambio, las sentencias ideales pueden ser tan complicadas como se quiera; ellas se unen con las sentencias reales sólo con el objetivo de sistematizar la teoría, para facilitar la deducción de sentencias reales. Por sí mismas, las sentencias ideales pueden incluso carecer de sentido informal.

Una teoría matemática permite deducir sentencias tanto ideales como reales. Sólo es importante que para esta teoría se cumpla el siguiente *principio de corrección*: toda sentencia real que se deduce en la teoría considerada es verdadera desde el punto de vista del sentido informal.

Demos un carácter más específico a esta idea. Consideremos la teoría axiomática formal ZF. Ésta es una teoría muy rica en posibilidades expresivas que trata con objetos muy complejos de investigación, entre los que se encuentran los conjuntos actualmente infinitos.

Como sabemos, la teoría Ar (aritmética formal) se interpreta en la teoría ZF. Consideremos en el lenguaje Ar la clase S formada por las sentencias de la forma

$$\forall x_1 \ldots x_n A(x_1, \ldots, x_n),$$

donde A es un *predicado decidible*. Por ejemplo, A puede tener la forma de la igualdad $(t = r)$ o una forma más compleja, pero en todo caso admite comprobación efectiva para números naturales concretos. Por ejemplo, es bien conocido que en el lenguaje Ar se puede construir una fórmula $A(n, x, y, z)$ con cuatro parámetros

que expresa naturalmente el predicado

$$x^{n+3} + y^{n+3} \neq z^{n+3}.$$

Entonces el Último teorema de Fermat,

$$\forall\, xyzn(x^{n+3} + y^{n+3} \neq z^{n+3}),$$

puede ser un elemento de S.

A cada sentencia $B \in S$ le corresponde una fórmula B^* del lenguaje ZF obtenida mediante la interpretación de B en el lenguaje ZF. Las fórmulas del tipo de B^* para $B \in S$ son las que denominaremos *sentencias reales* de ZF.

A las sentencias reales se les puede atribuir un sentido informal de manera natural. Si $B = \forall\, x_1, \ldots, x_n A(x_1, \ldots, x_n)$, entonces B es informalmente verdadera si, para todos los números naturales $m_1, \ldots, m_n$, el resultado de la verificación de la veracidad de la fórmula valorada $A(m_1, \ldots, m_n)$ siempre da que ella es verdadera. Esta definición de veracidad informal de las sentencias reales se expresa totalmente en el marco de los números naturales, no exige la utilización de conjuntos actualmente infinitos y utiliza solamente la abstracción de realizabilidad potencial: se exige que para todo conjunto realizable $m_1, \ldots, m_n$, el proceso de cálculo del valor de $A(m_1, \ldots, m_n)$ se pueda realizar hasta el final. El conjunto de todos los números naturales como conjunto actualmente realizable no se utiliza en este caso. El carácter elemental de esta definición está confirmado por la facilidad con que ella se formaliza en la teoría Ar. De esta manera, los medios lógicos utilizados para la definición de la veracidad informal de los enunciados reales, no provocan, por lo visto, la crítica expresada anteriormente.

Señalemos ahora un hecho importante. *Si la teoría* ZF *es consistente, ella satisface el principio de corrección, es decir, toda sentencia real deducible en* ZF *es informalmente verdadera.*

En efecto, supongamos que ZF es una teoría consistente. Tomemos un conjunto arbitrario de números $m_1, \ldots, m_n$ y calculemos el valor veritativo de $A(m_1, \ldots, m_n)$. Nosotros afirmamos que este valor es «verdad». En efecto, de otro modo el predicado decidible $\neg A$ tomaría el valor «verdad» en el conjunto $m_1, \ldots, m_n$. Con ayuda de un razonamiento extenso, pero sencillo en esencia (que utiliza la máquina de Turing de la definición del predicado decidible A), se puede demostrar que entonces en Ar se deduce $\neg A(\widetilde{m}_1, \ldots, \widetilde{m}_n)$ y, por tanto, $\exists\, x_1, \ldots, x_n \neg A(x_1, \ldots, x_n)$ (aquí, $\widetilde{m}_i$ es $S \ldots S0$, m_i veces), o bien $\neg \forall\, x_1, \ldots, x_n A(x_1, \ldots, x_n)$. Utilizando la interpretación en ZF, obtenemos la deducción de $\neg(\forall\, x_1, \ldots, x_n A(x_1, \ldots, x_n))^*$. Si $(\forall\, x_1, \ldots, x_n A(x_1, \ldots, x_n))^*$ fuera deducible en ZF, entonces ZF sería una teoría contradictoria.

Este razonamiento se puede aplicar a muchas otras teorías. De esta manera, la consistencia de la teoría considerada adquiere una importancia especial.

Señalemos también que un análisis cuidadoso muestra que la afirmación sobre la consistencia de ZF (y de muchas otras teorías) puede ser escrita como una afirmación *real*. Por eso, incluso si no estamos en condiciones de demostrar la consistencia de una teoría, podemos *entender* esta afirmación en cierto sentido informal y, por consiguiente, buscar bases informales para confiar o no confiar en ella.

3.4.4 ¿Cómo se puede demostrar la consistencia de una teoría?

Un método clásico aquí es el *método de interpretaciones*, con ayuda del cual el problema sobre la consistencia de una teoría se reduce a este mismo problema, pero respecto a otra teoría. De hecho este método apareció mucho antes de que comenzaran a desarrollarse los métodos exactos de descripción de teorías con ayuda de medios de la lógica matemática. La geometría analítica de Descartes (1619) puede ser considerada como una interpretación de la geometría con ayuda de medios del análisis. Cayley y Klein (1871) propusieron una conocida interpretación de la geometría de Lobachevski en la geometría de Euclides.

Desde el punto de vista moderno el método de interpretaciones consiste en la construcción de una interpretación relativa de una teoría axiomática formal en otra. En este caso, como hemos señalado, de la consistencia de la segunda teoría se deduce la consistencia de la primera.

Pero ¿cómo demostrar la consistencia de teorías potentes tales como ZF y la aritmética de orden superior, para las cuales es incluso difícil hallar una teoría matemática confiable para su argumentación?

Hilbert propuso un método de demostración de la consistencia que no exige la utilización directa de interpretaciones.

Señalemos que, aunque ZF describe una teoría compleja, la *formulación* de esta teoría axiomática formal exige medios muy elementales. Además, el propio concepto de consistencia de la teoría axiomática formal ZF es muy elemental y no necesita de conjuntos actualmente infinitos: la consistencia de ZF significa sencillamente que ninguna fila de símbolos del lenguaje ZF es deducción de una fórmula que tiene la forma $C \wedge \neg C$. Pero si la formulación del problema es tan elemental, podemos tener

la esperanza de que para demostrarlo sean suficientes medios también elementales, sin tener que profundizar en el contenido de la teoría, estudiando solamente la estructura formal de las deducciones de la teoría.

La esencia del programa de Hilbert de fundamentación de la matemática consiste en que primeramente la teoría estudiada debe ser formalizada y, seguidamente, se debe demostrar su consistencia con medios lógicos que no provoquen dudas, con métodos *finitos*.

Por ejemplo, la consistencia de ZF se puede expresar en el lenguaje Ar, por lo que se siente la tentación de deducir esta afirmación en la teoría formal Ar. Si esto fuera posible el problema sobre la consistencia de ZF se reduciría al problema sobre la consistencia de una teoría más simple, a saber, Ar.

Desgraciadamente, este programa es imposible realizar completamente. Como demostró Gödel en 1932, la consistencia de toda teoría suficientemente rica y efectivamente axiomatizada no puede ser demostrada utilizando medios de esta teoría.

De aquí se deduce, en particular, que la consistencia de ZF no puede ser demostrada incluso en ZF y, con mayor razón aún, no puede ser demostrada en Ar (por supuesto, si estas teorías son consistentes).

Para demostrar la consistencia de una teoría se deben utilizar medios lógicos suficientemente convincentes que no pueden ser formalizados en el marco de esta teoría. Estos medios lógicos deben tener un sentido intuitivo desde cierto punto de vista informal. Los medios lógicos necesarios han sido elaborados en el marco de las lógicas no clásicas y, sobre todo, en el *intuicionismo matemático* (véase [3]). En la actualidad la consistencia

de las teorías Ar y Ar2 se puede considerar demostrada convincentemente. La demostración de la consistencia de la teoría ZF es mucho más problemática.

Independientemente del problema de demostración de la consistencia, el método de formalización de las teorías matemáticas propuesto por Hilbert es el método central en la teoría moderna de las demostraciones.

Bibliografía

1. Bourbaki N. *Éléments de mathématique*. Livre I. Théorie des ensembles. Paris: Hermann, 1960.
2. Cohen P. J. *Set theory and the continuum hypothesis*. New York: Benjamin, 1966.
3. Dragalin A. G. *Intuicionismo matemático. Introducción a la teoría de la demostración*. Moscú: Naúka, 1979. Véase también: Dragalin A. G. *Teoría constructiva de la demostración y análisis no estándar*. Moscú: URSS, 2003 (en ruso).
4. Yershov Yu. L., Paliutin E. A. *Lógica matemática*. Moscú: Naúka, 1979 (en ruso).
5. Fraenkel A., Bar-Hillel Y. *Foundations of set theory*. Amsterdam: North-Holland, 1958.
6. Goodstein R. L. *Mathematical logic*. Leicester: Leicester University Press, 1957.
7. Hilbert D., Bernays P. *Grundlagen der Mathematik*. Berlin: Springer-Verlag, 1970.
8. Jech Th. J. *Lectures in set theory with particular emphasis on the method of forcing*. Berlin: Springer-Verlag, 1971.
9. Kleene S. C. *Introduction to metamathematics*. Amsterdam: Elsevier Science Ltd., 1971.
10. Kleene S. C. *Mathematical logic*. New York: Wiley, 1967.

11. Kolmogórov A. N., Dragalin A. G. *Lógica matemática. Introducción a la lógica matemática*. Moscú: URSS, 2014.
12. Lavrov I. A., Maxímova L. L. *Problemas de teoría de conjuntos, lógica matemática y teoría de algoritmos*. Moscú: Naúka, 1975 (en ruso).
13. Maltsev A. I. *Algorithms and recursive functions*. Groningen: Wolters-Noordhoff Pub. Co., 1970.
14. Mendelson E. *Introduction to mathematical logic*. New York: Van Nostrand Company Inc., 1964.
15. Novikov P. S. *Elements of mathematical logic*. Edinburgh: Oliver and Boyd, 1964.
16. Rogers H. *Theory of recursive functions and effective computability*. New York: McGraw Hill, 1967.
17. Shoenfield J. R. *Mathematical logic*. Reading: Addison-Wesley, 1967.
18. Takeuti G. *Proof theory*. Amsterdam: Elsevier Science Ltd., 1975.
19. Teoría matemática de la deducción lógica: Compendio de traducciones (recopilación de artículos traducidos al ruso). Moscú: Naúka, 1967 (en ruso).

Índice de autores*

Bar-Hillel, Y. 227
Bernays, P. 84, 227
Bernstein, F. 83
Bourbaki, N. 227

Cantor, G. 80, 81, 83, 215
Cayley, A. 224
Church, A. 10, 123–125
Cohen, P. 82, 83, 94–96, 227

De Morgan, A. 36, 37, 73, 76
Dragalin, A. G. 227, 228

Eubúlides 42
Euclides 107, 224

Fraenkel, A. 10, 44, 45, 85, 88, 219, 227

Gauss, J. 220
Gentzen, G. 11, 200, 203, 209
Gödel, K. 10, 82–84, 94, 96, 101, 124, 139, 152, 175, 176, 178, 179, 185, 187, 217, 225
Goodstein, R. L. 227

Herbrand, J. 124
Hilbert, D. 11, 86, 215, 220, 224, 225, 227
Horner, W. 108

Jech, Th. J. 227

Kleene, S. 155, 157, 167, 227
Klein, F. 224
Kolmogórov, A. N. 124, 228
Kuratowski, K. 51

Lavrov, I. A. 228
Löb, M. N. 181

* El índice de autores fue compuesto por Ye. G. Dragálina-Chórnaia.

Lobachevski, N. 224
Löwenheim, L. 10, 198

Máltsev, A. I. 197, 228
Márkov, A. A. 124
Maxímova, L. L. 228
Mendelson, E. 228

Nóvikov, P. S. 228

Paliutin, E. A. 227
Peano, G. 23, 24, 69, 70, 98, 99, 102, 103, 151
Post, E. 124, 134, 161, 163

Quine, W. 101

Rogers, H. 228
Rosser, J. B. 179
Russell, B. 41, 42, 48, 50, 81, 101

Schröder E. 83
Shoenfield, J. R. 228
Skolem, T. 10, 98, 198, 199

Takeuti, G. 228
Turing, A. 10, 11, 107, 109, 113, 114, 116–120, 122–125, 127–129, 134, 137, 138, 143, 146–148, 155, 156, 158–160, 162, 167, 223

Uspenski, V. A. 124

Von Neumann J. 67, 70, 84, 120

Whitehead, A. 101

Yershov, Yu. L. 227

Zermelo, E. 10, 44, 45, 85, 88, 219

Índice de materias*

Abstracción 30
— del infinito actual 220
— de enajenación 42
— de realizabilidad potencial 220
— ilimitada 30
alfabeto 110
— de estados 110
— de letras leídas 111
— externo 108, 110
— fundamental 145
— interno 110
— reducido 146
— simple 145
algoritmo 107
— de Kolmogórov—Uspienski 124
— de palabras 108
— normal de Márkov 124
aparición libre 12
— ligada 12
árbol de deducción 21
— de fórmulas 20
argumentación 22
aritmética de segundo orden 25
— elemental 23
axioma 102, 201
— del conjunto potencia 48, 89
— — vacío 47, 89
— del par 89
— — no ordenado 47
— de abstracción 25, 32
— de comprehensión 48, 55, 89
— de elección 82, 92, 94
— de extensionalidad 32, 46, 89
— de fundación 90
— de infinitud 89
— de la suma 47, 89
— de reemplazo 48, 89
— de regularidad 90
— no elemental 102
— — lógico 23, 24
axiomas del cálculo de predicados 19
— de igualdad 24
— de infinitud 48, 67

* El índice de materias fue compuesto por Ye. G. Dragálina-Chórnaia.

— de la teoría de conjuntos
de Zermelo—Fraenkel 45
— de Peano 24, 69, 99
— que definen la adición y
la multiplicación 24

Biyección 61
blanco 111

Cálculo de predicados puro 26
— de secuencias 202
— ecuacional
de Herbrand—Gödel 124
campo de una relación 53
Cantor, teorema 80
Cantor—Schröder—Bernstein,
teorema 83
categoricidad del conjunto de los
números naturales 98
— de una teoría 70
Church, definibilidad lambda 123
—, tesis 123, 124
clase 83, 84
— propia 84
colección de fórmulas 200
colisión de variables 15
complemento general 38, 50
composición de funciones 60
— de relaciones 56
computabilidad 127
concatenación de palabras 110
condición de uniformidad 59
conectiva lógica 13
configuración de cinta 111
— final 111
— inicial 111
conjunción 13
conjunto 29
— decidible de palabras 133
— de notaciones canónicas para los
números racionales 70
— de Russell 41, 48
— de todos los conjuntos 38
— — — números racionales 71
— — — subconjuntos 38
— — — — de números naturales 81
— finito 80
— infinito 39
— no computable 161
— — numerable 97
— numerable 80
— numerado de fórmulas 190
— potencia 38
— progresivo 39, 90
— recursivamente enumerable 129
— recursivo 128
— — de palabras 133
— relación 126
— unitario 33
— universal 38
— vacío 35
conjuntos equipotentes 80
— recursivamente inseparables 163
— — separables 163
consistencia de una teoría 87
— relativa de una teoría 94
constructivismo 101
continuidad 76, 218
— uniforme 76
convenios semánticos 48, 86
corte 203
— correcto 72

— en la región de los números racionales 72
cuantificador existencial 13
— limitado 36, 134
— universal 13

Decidibilidad 128
deducción 21
deducibilidad 200
definibilidad lambda de Church 123
definición de un conjunto por abstracción 30
— — — — comprehensión 40
— — — — reemplazo 40
— impredicativa 43
descripción recursiva primitiva (RP) 140
diferencia de conjuntos 35
disyunción 13
dominio de una relación 53

Elemento de turno 190, 191
enumerabilidad recursiva 129
enunciado paramétrico 14
espacio topológico 77
estado final 111
— inicial 111
estructura de Peano 98
Eubúlides, paradoja 42
exigencia estructural 21
expresión cerrada 12
— de un lenguaje 12
— valorada 16

Forma prenexa 19
— proposicional 14, 18
fórmula 12, 18, 29, 45
fórmula deducible 22
— en una teoría 23
función 58
— biunívoca 61
— característica 126
— computable 119, 120
— efectivamente computable 123
— incompletable 165
— no computable 162
— obtenida mediante la sustitución de una función en otra 157
— recursiva 120
— — parcial 120, 124
— — primitiva 140, 142
— — total 120, 143
— universal para una clase 158

Gödel, numeración 10, 149
—, número 146, 149
—, segundo teorema 178
—, teorema de incompletitud 176

Hilbert, método de formalización 86
hipótesis 21
— del continuo 81, 94

Imagen de un conjunto por una relación 58
— de una relación 54
implicación 13
— material 17
impredicatividad de la teoría de conjuntos 43
indecidibilidad de una teoría 182

instrucción 110
— inaplicable a una configuración K_1 112
— que transforma la configuración K_1 en K_2 114
interpretación 16
intersección de conjuntos 35
— de una familia de conjuntos 36, 64
introducción de variables subordinadas 74
intuicionismo matemático 225

Kleene, teorema de la forma normal 157
—, — de recursión 167
Kolmogórov—Uspienski, algoritmo 124

Lenguaje de la teoría ingenua de conjuntos 48
— de primer orden 13
— de una teoría 23
— explícitamente definido 136
letra de predicado 13
— de un alfabeto 110
— proposicional 13
ley lógica 18
lista de instrucciones 111
Löb, teorema 181
Löwenheim—Skolem, teorema 199

Máltsev, teorema de compacidad 197
máquina de Turing 113
— — reducida 146
metamatemática 100
método axiomático formal 103
— — informal 101
— de formalización de Hilbert 86
— de interpretaciones 224
modelo de una teoría 23
— no estándar 198
multiplicación de números racionales 71, 72

Negación 13
numeración de Gödel 10, 149
numeral 120
número de Gödel 146, 149, 159, 160
— natural 67

Objeto constructivo 108
operación de concatenación de palabras 110
— de minimización 156
— de sucesión 39
orden de una fórmula 190
— lineal 67

Palabra de máquina 111
— sobre un alfabeto 108, 110
par compatible de conjuntos 188
— completo de conjuntos 188
— no ordenado 32
— numerado de conjuntos 190
— ordenado 51
paradoja del mentiroso 42
— de Eubúlides 42
— de Russell 42
— de Skolem 10, 98, 199

paradojas de la teoría ingenua de conjuntos 29
parámetro de una expresión 12
Peano, axiomas 24, 69, 99
—, estructura 98
Post, teorema 134
predicado aritmético 127, 128
— decidible 127, 221
— de palabras 126
— monádico 139
— recursivamente enumerable 129
— recursivo 127
— — primitivo 143, 155, 164, 174
preimagen de un conjunto 58
premisa abierta 21
prescripción discreta 107
principio de corrección 221
— de inducción completa 24, 68
— — por pertenencia 91
problema decidible 162
— — de la parada 162
— de la parada 162
— general de la parada 163
— indecidible de la parada 162
producto cartesiano de dos conjuntos 55
— — de una familia de conjuntos 65
programa 111
— de Hilbert de fundamentación de la matemática 225
propiedad de aislamiento 109
— de determinación 109
— de generalidad 109
— de subfórmula 202
— de sustitución de igual por igual 32
protocolo de cálculo de una máquina de Turing 114

Rama de un árbol de fórmulas 21
rango de una relación 54
recursión primitiva 141
región de variación de una variable 16
regla de contracción 207
regla de generalización 20
regla invertible 209
relación 52
— definida en un conjunto 56
— de equivalencia 57
— inversa 56
— natural de equivalencia 71
— reflexiva 57
— simétrica 57
— transitiva 57
restricción de una relación a un conjunto 58
resultado de una sustitución correcta 15
Rosser, teorema de incompletitud 179
Russell, conjunto 41, 48
—, paradoja 42

Secuencia 22, 201
segundo teorema de Gödel 178
sentencia compatible con una teoría 88
— ideal 220
— independiente de una teoría 88
— real 220

símbolo de función 14
— lógico principal 15
singletón 33
sistema canónico de Post 124
Skolem, paradoja 10, 98, 199
sucesión fundamental de letras 145

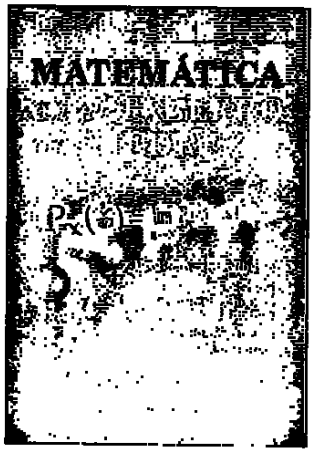
Tautología 18
técnica de deducción natural 22
teorema del punto fijo 173
— de admisibilidad del corte 209
— de Cantor 80
— de Cantor—Schröder—Bernstein 83
— de compacidad de Máltsev 197
— de completitud del cálculo de predicados 187, 197
— de deducción 22
— de eliminación del corte 202, 203
— de incompletitud de Gödel 176
— — de Rosser 179
— de indecidibilidad 183
— — del cálculo de predicados 186
— de la forma normal de Kleene 157
— de la función universal 158
— de Löb 181
— de Löwenheim—Skolem 199
— de Post 134
— de recursión de Kleene 167
— sobre la función incompletable 165
teoría ω-consistente 176
— axiomática de conjuntos de Zermelo—Fraenkel 88
— — explícitamente definida 138
— — formal 23
— categórica 70
— completa 88
— consistente 87, 175, 187
— decidible 139
— de conjuntos 31
— — de Quine 101
— de predicados monádicos 139
— de tipos 101
— elemental de los números reales 139
— indecidible 182, 183
— ingenua de conjuntos 48, 215
término 12, 29, 45
tesis de Church 123, 124
transitividad de un conjunto 91
Turing, máquina 113
—, — reducida 146

Unión de conjuntos 35
— de una familia de conjuntos 36, 64
universo 38, 84

Vacío (estado de una máquina de Turing) 111
valor de una función 59
— veritativo 223
variable libre 172
— proposicional 13
— subordinada 74

Zermelo—Fraenkel, teoría axiomática de conjuntos 88
n-tupla ordenada 52

EDITORIAL URSS



Ye. Yá. Guik

Matemática en el tablero de ajedrez

Tomo 1. **El tablero y las piezas**

Tomo 2. **Juegos matemáticos en el tablero de ajedrez**

Tomo 3. **La matemática de las puntuaciones y de los sistemas de torneos. Ajedrez computacional (el hombre y la computadora)**

La presente edición de la obra Matemática en el tablero de ajedrez, del conocido ajedrecista y escritor Yevgueni Guik, consta de tres tomos, a lo largo de los cuales se describen diversos puntos de contacto entre estas dos actividades del intelecto humano. Se resuelven diversos tipos de problemas matemáticos relacionados con el ajedrez: disección y recubrimiento del tablero, recorridos, disposiciones y permutaciones de las piezas (por ejemplo, el problema de Euler sobre el caballo y el problema de Gauss sobre las ocho damas). Se presentan diferentes récords matemático-ajedrecísticos y se describen las excepcionales propiedades geométricas del tablero. Se presta gran atención a los juegos recreativos, lógicos y matemáticos que se pueden desarrollar en el tablero de ajedrez. Se analizan problemas de ajedrez fantástico (problemas de fantasía) con la participación de las llamadas piezas mágicas. Se investigan los juegos en tableros no habituales, con reglas inusuales y piezas insólitas: ajedrez cilíndrico, proyectivo y hexagonal, el ajedrez aleatorio de Fischer y muchos otros. Se consideran los problemas matemáticos que surgen en la organización de los torneos de ajedrez, así como el sistema de puntuación que se emplea para valorar la fuerza de los jugadores. Se dedica gran atención a los logros de la computación en el juego práctico, en el análisis de finales, en la solución de problemas y finales artísticos. Este libro será útil e interesante para todos los aficionados al ajedrez, a la matemática (de cualquier nivel) y la ciencia computacional, así como para los amantes de los juegos intelectuales y pasatiempos matemáticos.

Medviédev G. N.

Problemas de matemática. Olimpiadas y exámenes de admisión. Facultad de Física de la Universidad Lomonósov de Moscú

El presente libro pretende familiarizar a estudiantes preuniversitarios y profesores con los exámenes de matemática que se han de superar para la admisión en la Facultad de Física de la Universidad Lomonósov de Moscú. Se recopilan las pruebas propuestas en 60 exámenes y olimpiadas de matemática que tuvieron lugar en dicho centro entre los años 1971 y 2006; cada prueba se presenta en dos variantes diferentes. Todos los problemas van acompañados de sus respectivas respuestas.

En la segunda parte del libro se ofrece la solución detallada de los problemas geométricos y algebraicos de mayor dificultad; además, los problemas que aquí se resuelven no coinciden con los de las variantes ofrecidas en la primera parte (es decir, son una tercera variante del mismo examen). De este modo, el estudiante en cada caso tiene a su disposición dos variantes completas no resueltas de cada examen y las indicaciones para la superación de las mismas, dadas en la segunda parte del libro al resolverse los problemas de mayor dificultad similares a los propuestos en dichas dos variantes.

Este libro está especialmente dirigido tanto a los estudiantes preuniversitarios que se preparan para los exámenes de admisión en centros de educación superior, como a los profesores especializados en esta labor.

Boss V.

Lecciones de matemática en 20 tomos

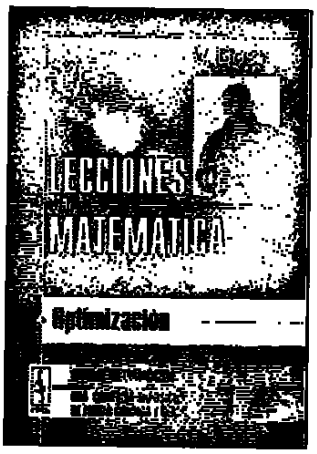
La gran avalancha de información que nos abruma hoy hace que los instrumentos del ayer dejen de desempeñar su función. Por esta razón, es necesario aprender a estudiar de una nueva forma; no porque el material a asimilar haya aumentado demasiado, sino porque en la vida han aparecido muchos otros temas de interés; por este motivo, casi nadie está dispuesto a dedicarle mucho tiempo a algo en particular. La serie «Lecciones de Matemática» pretende ser un experimento en esta dirección. El tiempo dirá si es acertado o no. De todos modos, esta serie es un producto de nueva generación: las mismas «ruedas», el mismo «volante», el mismo contenido matemático, pero con un aspecto diferente.

La idea central de esta serie es la economía de palabras y de medios. Tras las declaraciones de brevedad y claridad, es verdad que los 20 tomos planificados pueden causar una impresión diametralmente opuesta, pero esa considerable cantidad se debe no al exceso de detalles, sino a la formidable extensión de la matemática.

Los libros de esta serie se caracterizan por una exposición breve y clara de los temas tratados, valiéndose de analogías y sin entrar en detalles no estrictamente necesarios. Se presta especial atención a la interrelación de los resultados y al enfoque general del material considerado. En definitiva, se ha intentado crear un libro no sujeto a rutina, que ofrezca una imagen general, muestre los motivos, los enlaces, nos diga para qué es necesaria cada cosa.

La obra está dirigida a estudiantes universitarios, profesores, ingenieros y cientfficos.

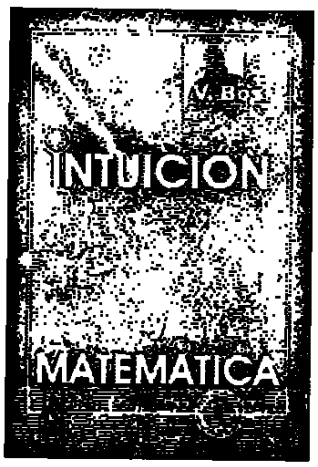
Tomo 1. **Análisis;** *Tomo 2.* **Ecuaciones diferenciales;** *Tomo 3.* **Álgebra lineal;** *Tomo 4.* **Probabilidad, información, estadística;** *Tomo 5.* **Análisis funcional;** *Tomo 6.* **Lógica, algoritmos, computabilidad. De Diofanto a Turing y Gödel.** *Tomo 7.* **Optimización;** *Tomo 8.* **Teoría de grupos;** *Tomo 9.* **Teoría de funciones de variable compleja;** *Tomo 10.* **Búsqueda exhaustiva y algoritmos eficientes;** *Tomo 11.* **Ecuaciones de la física matemática;** *Tomo 12.* **Contraejemplos y paradojas;** *Tomo 13.* **Topología;** *Tomo 14.* **Teoría de números.**



Boss V.

Lecciones de Matemática: Optimización

El presente libro se caracteriza por una exposición breve y clara de los temas tratados, valiéndose de analogías y sin entrar en detalles innecesarios. Se presta especial atención a la interrelación de los resultados y al enfoque general del material considerado. En este tomo de la serie se tratan los capítulos clásicos de la teoría de problemas de extremo: optimización condicionada y no condicionada, programación convexa, cálculo variacional, principio del máximo, programación dinámica. Se estudian también algunas áreas no tradicionales de la optimización, como son las bifurcaciones, las catástrofes, la teoría de juegos, los problemas de control óptimo y la optimización no suave. Merecen ser mencionados aparte los métodos de agregación asintótica para los problemas de grandes dimensiones. La exposición del material se caracteriza por ser concisa y clara. Esta obra está dirigida a estudiantes, profesores, ingenieros y cientfficos.



Boss V.

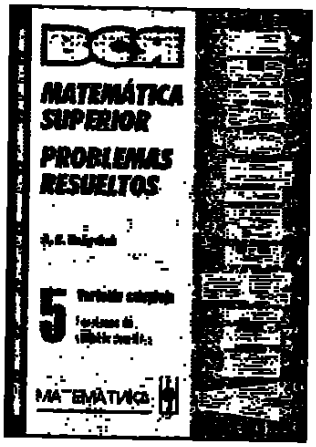
Intuición y matemática

El presente libro pone al descubierto la esencia de muchas ideas matemáticas, y constituye, evidentemente, un nuevo paso en el campo de la popularización de las ciencias. De manera inesperadamente sencilla y breve se transmite el sentido de muchos resultados fundamentales: hechos complejos se presentan en una forma clara a nivel intuitivo; el estilo de la exposición es inusualmente económico; la entonación, familiar.

Esta obra está dirigida a un amplio círculo de lectores, fundamentalmente a estudiantes universitarios, profesores e investigadores. También puede ser útil para los estudiantes de enseñanza media que sean capaces de «evitar» los elementos de matemática superior dispersos por el libro.

Boiarchuk A. K., Liashko I. I., Gai Ia. G., Golovach G. P.

AntiDemidóvich. Matemática superior. Problemas resueltos



Tomo 1. **Análisis matemático: introducción al análisis; cálculo diferencial para funciones de una variable;**
Tomo 2. **Análisis matemático: cálculo integral para funciones de una variable;**
Tomo 3. **Análisis matemático: series; funciones de argumento vectorial;**
Tomo 4. **Análisis matemático: integrales múltiples y curvilíneas;**
Tomo 5. **Variable compleja: funciones de variable compleja;**
Tomo 6. **Variable compleja: integración y series;**
Tomo 7. **Variable compleja: residuos y temas especiales;**
Tomo 8. **Ecuaciones diferenciales: ecuaciones diferenciales de primer orden;**
Tomo 9. **Ecuaciones diferenciales: ecuaciones diferenciales de órdenes superiores, sistemas de ecuaciones diferenciales y ecuaciones en derivadas parciales;**
Tomo 10. **Ecuaciones diferenciales: estabilidad y temas especiales**

La colección «AntiDemidóvich» que proponemos al lector abarca casi todas las ramas de las matemáticas.

Los cuatro primeros tomos con los que se abre esta obra, están dedicados al estudio práctico de las funciones, las sucesiones, las series, el cálculo diferencial e integral de las funciones de una y varias variables; en ellos se presentan soluciones completamente detalladas de los problemas expuestos en el famoso libro de B. P. Demidóvich.

En «Variable compleja» se resuelven detalladamente casi cuatrocientos problemas de dificultad media o alta.

Tomo 5: Este tomo incluye un repaso de las estructuras fundamentales del análisis matemático, números complejos, funciones de variable compleja y un estudio detallado de las funciones elementales en el plano complejo.

Tomo 6: Este tomo incluye integración en el plano complejo, integral de Newton—Leibniz, integral de Cauchy, series de funciones analíticas, puntos singulares aislados y prolongación analítica.

Tomo 7: Este tomo incluye teoría de los residuos, funciones enteras y meromorfas, productos infinitos, aplicación de los residuos al cálculo de integrales y sumas de series, y algunas cuestiones generales de la teoría geométrica de las funciones analíticas.

En «Ecuaciones diferenciales» se resuelven detalladamente casi ochocientos problemas de dificultad media o alta, y se proponen más de trescientos problemas como ejercicios de autocontrol (con sus respectivas soluciones). Cada sección va acompañada de un mínimo teórico estrictamente necesario para la resolución de los problemas correspondientes.

Tomo 8: En este tomo, se estudian las ecuaciones diferenciales de primer orden; el tomo contiene 251 problemas detalladamente resueltos.

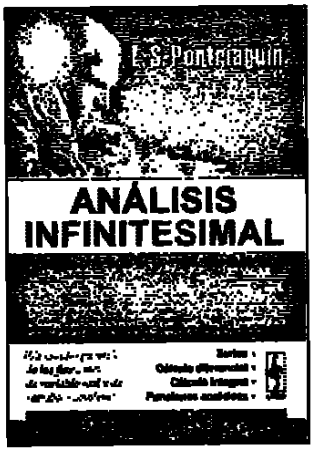
Tomo 9: En este tomo, se estudian las ecuaciones diferenciales de órdenes superiores, los sistemas de ecuaciones diferenciales y las ecuaciones en derivadas parciales de primer orden; el tomo contiene 273 problemas detalladamente resueltos.

Tomo 9: En este tomo, se estudian las ecuaciones diferenciales de órdenes superiores, los sistemas de ecuaciones diferenciales y las ecuaciones en derivadas parciales de primer orden; el tomo contiene 273 problemas detalladamente resueltos.

Tomo 10: En este tomo, se analizan diversos métodos de resolución aproximada de ecuaciones diferenciales, estabilidad y trayectorias de fase; se estudia, asimismo, el método de las transformaciones integrales de Laplace para la resolución de las ecuaciones diferenciales lineales; el tomo contiene 244 problemas detalladamente resueltos.

Pontriaguin L. S.

Primera Cita con la Matemática Superior



Tomo 1. **Análisis infinitesimal;**
Tomo 2. **Ecuaciones diferenciales y sus aplicaciónes;**
Tomo 3. **Método de coordenadas;** *Tomo 4.* **Álgebra**

Esta serie fue ideada por el eminente matemático soviético Liev Semiónovich Pontriaguin (1908–1988). Su objetivo es familiarizar a los jóvenes con la matemática superior ya antes de ingresar en la universidad, y está perfectamente resumido en las siguientes palabras de su autor: «*Estos libros están dedicados al estudio de los resultados más importantes de la matemática superior clásica. La elección del material y el orden en que éste se imparte no corresponden a ningún programa de estudios. Los libros reflejarán mis preferencias y mi punto de vista personal sobre la matemática formados en el transcurso de muchos años de trabajo. Además, tendrán en cuenta mis propios recuerdos sobre las posibilidades de percepción de los jóvenes, a fin de que las nuevas generaciones, a partir ya de los últimos cursos de la escuela, puedan familiarizarse con la matemática superior, y adquirir desde un principio un gusto sano y correcto respecto a la misma. La atención del lector debe estar dirigida no a refinamientos teóricos como, por ejemplo, la teoría de conjuntos o la teoría de límites, sino a los resultados matemáticos principales que se formaron en el transcurso de milenios*».

Se recomienda a los estudiantes preuniversitarios que se interesan por la matemática, así como a los estudiantes de los primeros cursos de institutos de enseñanza superior. Puede ser de interés para los profesores de enseñanza media y superior.

Pontriaguin L. S.

Generalizaciones de los números

En el presente libro se exponen de una manera asequible las posibles generalizaciones del concepto de número. Primero se analizan detalladamente las generalizaciones de los números reales, concretamente, los números complejos y los cuaterniones. Se demuestra que, salvo los números reales y los complejos, en la matemática no existen otras magnitudes lógicamente posibles, análogas a los reales y a los complejos, que puedan desempeñar el papel de números. Finalmente se consideran otras generalizaciones del concepto de número, pero que no contienen a los números reales.

Sus opiniones, sugerencias y proposiciones pueden ser enviadas a:

Rusia, 117335 Moscú
Nakhimovsky Prospekt, 56.

Grupo URSS

e-mail: URSS@URSS.ru
http://URSS.ru

o bien a nuestro distribuidor exclusivo en España:

España, 41960-Gines (Sevilla)
Pol. Servialsa, Calle B, №24

HAYKA LIBROS

e-mail: HAYKA@haykalibros.es
tel./fax: +34 (954) 71 98 62
móvil: +34 (625) 37 87 73

Московский государственный университет имени М. В. Ломоносова

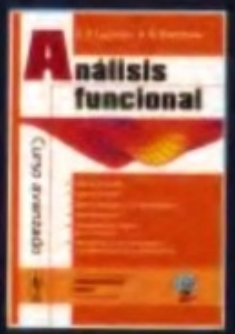
КЛАССИЧЕСКИЙ УНИВЕРСИТЕТСКИЙ УЧЕБНИК

Andréi Nikoláievich Kolmogórov

Eminente matemático soviético, miembro de la Academia de Ciencias de la Unión Soviética. Nació el 25 de abril de 1903 en la ciudad de Tambov (Rusia). En 1925 concluyó sus estudios en la Primera Universidad de Moscú (célebre institución que, posteriormente, se convertiría en la actual Universidad Estatal «M. V. Lomonósov» de Moscú), donde trabajó como profesor desde 1931. Ejerció el cargo de jefe de varios departamentos y decano de la Facultad de Mecánica y Matemática de esta universidad. Autor de numerosos trabajos considerados clásicos en la teoría de funciones de variable real, teoría de conjuntos, topología, lógica constructiva, análisis funcional, mecánica teórica, teoría de algoritmos, teoría de la información, etcétera. Los resultados logrados por Kolmogórov en la teoría de probabilidades tienen carácter fundamental. Es bien conocida su actividad relacionada con la metodología y la organización de la enseñanza de la matemática. Ocupó el cargo de presidente de la Sociedad Matemática de Moscú. Doctor *honoris causa* de numerosas universidades extranjeras, miembro de diferentes academias y sociedades científicas, galardonado con premios internacionales y órdenes estatales.

Albert Grigórievich Dragalin

Destacado representante de la escuela soviética de constructivismo matemático. Nació el 10 de abril de 1941 en la isla Morzhebiets (Región de Arjánguelsk, Rusia). Estudió en la Facultad de Mecánica y Matemática de la Universidad Estatal «M. V. Lomonósov» de Moscú, donde trabajó desde 1966. Desde 1983 vivió en Hungría. Dirigió el Departamento de Matemática de Cálculo de la Universidad «L. Kossuth» de la ciudad de Debrecen. La Academia de Ciencias de Hungría le otorgó el título de Doctor en Ciencias en 1988. Autor de trabajos fundamentales sobre los fundamentos de la teoría de modelos y la teoría de la demostración en la lógica intuicionista, y sobre los métodos constructivos en el análisis no estándar.



7989 ID 108167

9 785396 000728 >

URSS Scientific Books

RUSSIA • MOSCOW

URSS@URSS.ru

Phone/fax: + 7 (499) 724 25 45

URSS

HAYKA

LIBROS DE CIENCIA

Distribuidor exclusivo en España de Grupo URSS

• e-mail: HAYKA@haykalibros.es
• tel./fax: + 34 (954) 71 98 62
• móvil: + 34 (625) 37 87 73

Estamos a su disposición en URSS@URSS.ru; todo tipo de sugerencias, erratas y otros pormenores serán expuestos en la página web de este libro que figura en nuestra librería virtual

http://URSS.ru